



Cisco Service Control Application for Broadband User Guide

Version 3.0
OL-7205-02

Corporate 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: 408 526-4100

Customer Order Number: OL-7205-02
Text Part Number: OL-7205-02



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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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

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

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Printed in the USA on recycled paper containing 10% postconsumer waste.

Cisco SCA BB User Guide

Copyright © 2002-2005 Cisco Systems, Inc.
All rights reserved.



Preface ix

- Document Revision History ix
- Audience x
- Organization x
- Related Documentation xi
- Conventions xi
- Obtaining Documentation xii
 - World Wide Web xii
 - Documentation CD-ROM xiii
 - Ordering Documentation xiii
 - Documentation Feedback xiii
- Obtaining Technical Assistance xiii
 - Cisco.com xiv
 - Technical Assistance Center xiv

Overview 1-1

- The Cisco Service Control Concept 1-1
 - Cisco Service Control Application for Broadband - Service Control for Broadband Service Providers 1-2
- Service Control Capabilities 1-2
- The SCE Platform 1-3
- Management and Collection 1-4
 - Network Management 1-5
 - Subscriber Management 1-5
 - Service Configuration Management 1-5
 - Collection 1-5

System Overview 2-1

- System Components 2-1
- Subscribers and Subscriber Modes 2-3

- Subscriberless Mode 2-3
- Anonymous Subscriber Mode 2-4
- Static Subscriber Mode 2-4
- Subscriber-Aware Mode: Dynamic Subscribers 2-4
- Subscriber Modes: Summary 2-5
- Service Configuration 2-5
 - The SCAS BB Console 2-6
 - The SCA BB Service Configuration Utility 2-6
 - Service Configuration API 2-6

Traffic Processing Overview 3-1

- Traffic Classification 3-1
 - Services 3-2
 - Protocols 3-4
 - Initiating Side 3-5
 - Zones 3-5
 - Flavors 3-6
 - Mapping Flow Attributes to Services 3-7
- Traffic Accounting and Reporting 3-7
 - Usage Accounting 3-7
 - RDRs 3-9
- Traffic Control 3-10
 - Packages 3-10
 - Unknown Subscriber Traffic 3-10
 - Rules 3-11
 - Bandwidth Management 3-11
 - Quota Management 3-15
- Other Traffic Processing Features 3-16
 - Traffic Filters 3-16
 - Traffic Forwarding to VAS Servers 3-16
- Service Configurations 3-16
 - Defining Service Configurations in Practice 3-17

Getting Started 4-1

- Installing SCA BB 4-1

- Prerequisites 4-2
- The SCA BB Installation Package 4-3
- Installing SCA BB Application Components 4-3
- Installing SCA BB Front Ends 4-4
- Installing Protocol Packs 4-8
- Upgrading from Version 2.5 to Version 3.0 4-13
 - Upgrading the SCA BB Service Configuration Utility 4-14
- Launching the SCAS BB Console 4-14
- Using the SCAS BB Console 4-16
 - Navigating in the SCAS BB Console 4-16
 - Accessing On-Line Help 4-22
- Quick Start with the SCAS BB Console 4-23

Using the Network Navigator 5-1

- The Network Navigator Tool 5-1
- Managing Sites 5-2
 - Adding a Site to the Site Manager 5-2
 - Adding Devices to a Site 5-3
 - Deleting Sites 5-6
- Managing Devices 5-6
 - Managing SCE Devices 5-6
 - Managing SM Devices 5-15
 - Managing CM Devices 5-19
 - Managing Database Devices 5-20
- Password Management 5-24
- Working with Network Navigator Configuration Files 5-24
 - Exporting a Network Navigator Configuration 5-25
 - Importing a Network Navigator Configuration 5-27
- Network Settings Requirements 5-29
 - Firewall/NAT Requirements 5-29
 - User Authentication 5-29

Using the Service Configuration Editor 6-1

- The Service Configuration Editor Tool 6-1
- Managing Service Configurations 6-2

- Adding New Service Configurations 6-2
- Opening Existing Service Configurations 6-3
- Saving the Current Service Configuration 6-4
- Closing Service Configurations 6-5
- Exporting Service Configuration Data 6-5
- Importing Service Configuration Data 6-9
- Applying and Retrieving Service Configurations 6-13

Using the Service Configuration Editor: Traffic Classification 7-1

- Managing Services 7-1
 - Service Parameters 7-2
 - Viewing Services 7-2
 - Adding Services 7-4
 - Editing Services 7-8
 - Deleting Services 7-9
 - Managing Service Elements 7-10
- Managing Protocols 7-20
 - Viewing Protocols 7-21
 - Adding Protocols 7-23
 - Editing Protocols 7-24
 - Deleting Protocols 7-25
 - Managing Protocol Elements 7-26
 - Managing Protocol Signatures: Dynamic Signatures 7-32
- Managing Zones 7-42
 - Viewing Zones 7-42
 - Adding Zones 7-43
 - Editing Zones 7-44
 - Deleting Zones 7-44
 - Managing Zone Items 7-45
- Managing Flavors 7-48
 - Flavor Types and Parameters 7-48
 - Viewing Flavors 7-48
 - Adding Flavors 7-50
 - Editing Flavors 7-51

Deleting Flavors 7-51
Managing Flavor Items 7-52

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

Managing Usage Counters 8-1
Managing RDR Settings 8-1
 Managing Usage RDRs 8-2
 Managing Transaction RDRs 8-4
 Managing Quota RDRs 8-6
 Managing Transaction Usage RDRs 8-8
 Managing Log RDRs 8-10
 Managing Real-Time Subscriber Usage RDRs 8-12
 Managing Real-Time Signaling RDRs 8-14

Using the Service Configuration Editor: Traffic Control 9-1

Managing Packages 9-1
 Package Parameters 9-1
 Viewing Packages 9-2
 Adding Packages 9-4
 Duplicating Packages 9-7
 Editing Packages 9-8
 Deleting Packages 9-9
Unknown Subscriber Traffic 9-10
Managing Rules 9-11
 Viewing the Rules of a Package 9-11
 The Default Service Rule 9-12
 Rule Hierarchy 9-12
 Adding Rules to a Package 9-12
 Editing Rules 9-17
 Deleting Rules 9-19
 Displaying the Services Affected by a Rule 9-20
 Managing Time-Based Rules 9-21
 Managing Calendars 9-26
Managing Bandwidth 9-31
 Managing Global Bandwidth 9-31

- Viewing Global Controller Settings 9-31
- Editing the Total Link Limits 9-34
- Adding Global Controllers 9-34
- Editing Global Controllers 9-35
- Deleting Global Controllers 9-35
- Defining Global Controllers in a Dual Link System 9-36
- Managing Subscriber Bandwidth 9-39
- Managing Bandwidth: a Practical Example 9-42
- Setting BW Management Prioritization Mode 9-46
- Managing Quotas 9-48
 - Editing Package Quota Management Settings 9-48
 - Selecting Quota Buckets for Rules 9-49
 - Editing Breach Handling Parameters for a Rule 9-51
- Using the Service Configuration Editor: Additional Options 10-1**
 - Filtering the Traffic Flows 10-1
 - Viewing Filter Rules 10-2
 - Adding Filter Rules 10-2
 - Editing Filter Rules 10-7
 - Deleting Filter Rules 10-8
 - Activating and Deactivating Filter Rules 10-9
 - Managing Subscriber Notifications 10-9
 - Subscriber Notification Parameters 10-9
 - Viewing Subscriber Notifications 10-11
 - Adding Subscriber Notifications 10-12
 - Editing Subscriber Notifications 10-13
 - Deleting Subscriber Notifications 10-13
 - Managing the System Settings 10-14
 - Setting the Operational Mode of the System 10-14
 - Setting Redirection Parameters 10-16
 - Managing Advanced Service Configuration Options 10-21
 - Managing VAS Traffic Forwarding Settings 10-23
 - VAS Traffic Forwarding and Bandwidth Management 10-23
 - Enabling VAS Traffic Forwarding 10-24

- Renaming VAS Server Groups 10-25
- Viewing VAS Traffic Forwarding Tables 10-26
- Adding VAS Traffic Forwarding Tables 10-27
- Deleting VAS Traffic Forwarding Tables 10-27
- Managing VAS Table Parameters 10-28

Using the Subscriber Manager GUI Tool 11-1

- The SM GUI Tool 11-1
 - Connecting to an SCMS-SM 11-2
- Working with Subscriber CSV Files 11-5
 - Importing Subscriber Files 11-5
 - Exporting Subscriber Files 11-6
- Managing Subscribers 11-7
 - Subscriber Information 11-7
 - Finding and Selecting Subscribers 11-7
 - Adding Subscribers 11-9
 - Editing Subscribers 11-11
 - Deleting Subscribers 11-13

Using the Signature Editor 12-1

- Managing DSS Files 12-1
 - DSS File Components 12-1
 - Creating DSS Files 12-9
 - Editing DSS Files 12-12
 - Importing Signatures 12-13
 - The Signature Editor Console 12-15

Additional Management Tools and Interfaces 13-1

- The Cisco Service Control Application for Broadband Service Configuration Utility 13-1
 - Using the SCA BB Service Configuration Utility 13-1
 - SCA BB Service Configuration Utility Examples 13-3
- The SCA BB Signature Configuration Utility 13-4
 - Using the SCA BB Signature Configuration Utility 13-4
 - SCA BB Signature Configuration Utility Examples 13-4
- Attack Filtering and Subscriber Notification 13-5

- Subscriber Notification on Network Attack 13-5
- SNMP, MIB, and Traps: Overview 13-11
 - SNMP 13-11
 - MIB 13-12
 - Traps 13-12
- Managing Subscribers via Other System Components 13-12
 - Anonymous-Subscriber Mode 13-13
 - Subscriber-Aware Mode 13-14
 - Selecting Subscribers for Real-Time Usage Monitoring 13-15
 - Managing CSV Files 13-18
- Glossary of Terms GL-1**
- Index I-1**



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

Cisco Service Control Release	Part Number	Publication Date
Release 3.0.0	OL-7205-02	December, 2005

DESCRIPTION OF CHANGES

Both the look-and-feel and the functionality of the Service Control Application Suite for Broadband (SCAS BB) Console were redesigned for version 3.0; consequently, this document underwent a major rewrite. The major changes in this document include:

- 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 SCAS BB Console: the Network Navigator tool and the Signature Editor tool

Release 2.5.5	OL-7205-01	February, 2005
---------------	------------	----------------

DESCRIPTION OF CHANGES

Created the *Cisco Service Control Application for Broadband User Guide*.

Audience

This guide is intended for the administrator who is responsible for daily operation of the Cisco Service Control solution, using the many features of the SCAS BB Console, the Cisco Service Control Management Suite (SCMS) Subscriber Manager (SM), and the Cisco Service Control Application Suite Reporter front ends to gain visibility into, and control over, the distribution of network resources.

Organization

This guide is organized as follows:

The major sections of this guide are as follows:

Chapter	Title	Description
Chapter 1	<i>Overview</i> (on page 1-1)	Provides a general overview of the Cisco Service Control solution
Chapter 2	<i>System Overview</i> (on page 2-1)	Provides a functional overview of the Cisco Service Control solution
Chapter 3	<i>Traffic Processing Overview</i> (on page 3-1)	Provides a technical overview of the Cisco Service Control solution
Chapter 4	<i>Getting Started</i> (on page 4-1)	Guides you through the process of installing or upgrading SCA BB and describes the notion of the SCAS BB Console as a collection of tools
Chapter 5	<i>Using the Network Navigator</i> (on page 5-1)	Explains how to use the Network Navigator to create a model of all devices that are part of the Cisco Service Control solution and how to manage the devices remotely
Chapter 6	<i>Using the Service Configuration Editor</i> (on page 6-1)	Explains how to use the Service Configuration Editor to manage service configurations
Chapter 7	<i>Using the Service Configuration Editor: Traffic Classification</i> (on page 7-1)	Explains how to configure service configurations to perform traffic classification
Chapter 8	<i>Using the Service Configuration Editor: Traffic Accounting and Reporting</i> (on page 8-1)	Explains how to configure service configurations to perform traffic reporting
Chapter 9	<i>Using the Service Configuration Editor: Traffic Control</i> (on page 9-1)	Explains how to configure service configurations to perform traffic control
Chapter 10	<i>Using the Service Configuration Editor: Additional Options</i> (on page 10-1)	Documents additional, advanced options available in the Service Configuration Editor
Chapter 11	<i>Using the Subscriber Manager GUI Tool</i> (on page 11-1)	Explains how the SM GUI tool can be used to configure subscribers on the SCMS-SM database
Chapter 12	<i>Using the Signature Editor</i> (on page 12-1)	Documents the Signature Editor tool that can create files for updating protocols in SCA BB

Chapter 13	<i>Additional Management Tools and Interfaces</i> (on page 13-1)	Documents and explains other tools that are available for use with SCA BB
------------	---	--

Related Documentation

The following publications are available for the *Cisco Service Control Application for Broadband*:

- *Cisco Service Control Application for Broadband Reference Guide*
- *Cisco Service Control Application for Broadband Service Configuration API Programmer's Guide*
- *Cisco Service Control Management Suite Collection Manager User Guide*
- *Cisco Service Control Management Suite Subscriber Manager User Guide*
- *Cisco Service Control Application Suite 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 CLI Command Reference*
- *Cisco Service Control Engine Software Configuration Guide*

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{x y z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .

→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control —for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Non printing 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.

Notes use the following conventions:



Note

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

Cautions use the following conventions:



Caution

Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Warnings use the following conventions:



Warning

Means *reader be warned*. You are capable of doing something that might result in bodily injury.

Obtaining Documentation

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

World Wide Web

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

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

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

Documentation Feedback

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

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

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

Attn Document Resource Connection

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides *Cisco.com* (on page [xiv](#)) as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

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

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

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

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

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

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

To register for *Cisco.com* (on page [xiv](#)), go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

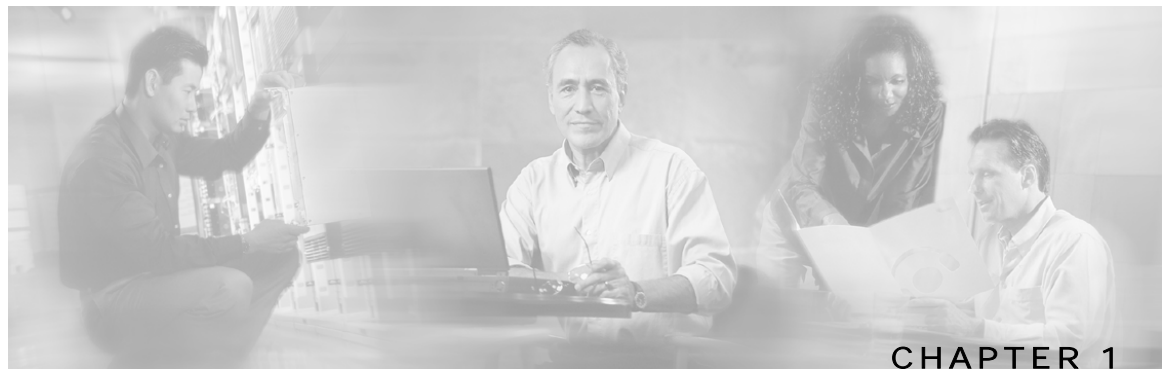
Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

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



Overview

This chapter provides a general overview of the Cisco Service Control solution. It introduces the Cisco Service Control concept and the Service Control capabilities. It also briefly describes the hardware capabilities of the Service Control Engine (SCE) platform, as well as the Cisco specific applications that together compose the total Cisco Service Control solution.

This chapter contains the following sections:

- [The Cisco Service Control Concept](#) 1-1
- [Service Control Capabilities](#) 1-2
- [The SCE Platform](#) 1-3
- [Management and Collection](#) 1-4

The Cisco Service Control Concept

The Cisco Service Control solution is delivered through a combination of purpose-built hardware and specific software solutions that address various Service Control challenges faced by service providers. The SCE platform is designed to support classification, analysis, and control of Internet/IP traffic.

Service Control enables service providers to create profitable new revenue streams while capitalizing on their existing infrastructure. With the power of Service Control, service providers have the ability to analyze, charge for, and control IP network traffic at multi-Gigabit wire line speeds. The Cisco Service Control solution also gives service providers the tools they need to 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 rising costs. At the same time, access and bandwidth have become a commodity 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. However, capturing real profits from IP services requires more than simply running those services over data links; it requires detailed monitoring and precise, real-time control and awareness of services as they are delivered. Cisco provides Service Control solutions that allow the service provider to bridge this gap.

Cisco Service Control Application for Broadband - 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 (Engage)* adds a new 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 SLAs
- Implement different service levels for different types of customers, content, or applications
- Identify network abusers who are violating the Acceptable Use Policy
- Identify and manage peer-to-peer, NNTP (news) traffic, and spam abusers
- Enforce the Acceptable Use Policy (AUP)
- Integrate Service Control solutions easily with existing network elements and BSS/ OSS systems

Service Control Capabilities

At the core of the Cisco Service Control solution stands the purpose-built network hardware device: the Service Control Engine (SCE). The core capabilities of the SCE, 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 for maintaining the state of each subscriber transmitting traffic through the SCE platform, and enforcing the appropriate policy on this subscriber's traffic

Subscriber awareness is achieved using dedicated integrations with subscriber management repositories, such as a DHCP or a Radius server, or via 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 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 easily adapt to new services and applications in the ever-changing service provider environment. Programmability is achieved using the Cisco Service Modeling Language (SML).

Programmability is required for new services to be deployed quickly, and it 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 and robust integration process.
- Scalable high-performance service engines—The ability to perform all these operations at wire speed.

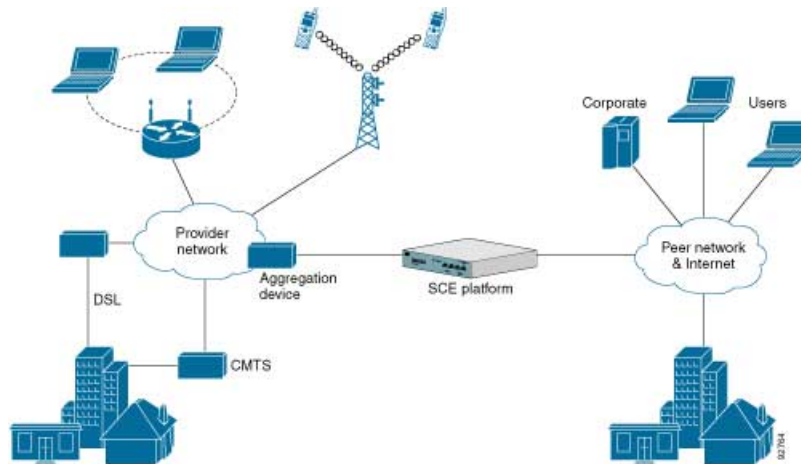
The SCE Platform

The SCE family of programmable network devices is capable of performing application-layer stateful-flow inspection of IP traffic, and controlling that traffic based on configurable rules. The SCE is a purpose-built network device that uses ASIC components and RISC processors to go beyond packet counting and delve deeper into the contents of network traffic. Providing programmable, stateful inspection of bidirectional traffic flows and mapping these flows with user ownership, the SCE platforms provide a real-time classification of network usage. This information provides the basis of the SCE advanced traffic-control and bandwidth-shaping functionality. Where most bandwidth shaper functionality ends, the SCE provides more control and shaping options including:

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

The following diagram illustrates a common deployment of an SCE platform in a network.

Figure 1-1: SCE Platform in the Network



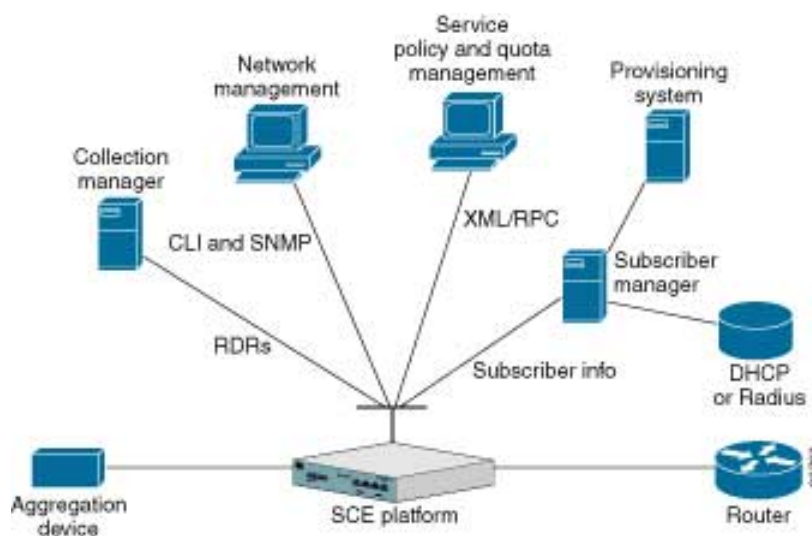
Management and Collection

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 easily integrate with existing OSS infrastructure.

Figure 1-2: Service Control Management Infrastructure



Network Management

Cisco provides complete network FCAPS (Fault, Configuration, Accounting, Performance, Security) Management.

Two interfaces are provided for network management:

- Command-Line Interface (CLI)—The CLI is accessible through the Console port or through a Telnet connection; it is used for configuration and security functions
- SNMP—SNMP provides fault management via SNMP traps, as well as performance monitoring functionality

Subscriber Management

In cases where *SCA BB* is used to enforce different 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 the OSS and the SCE platforms. Subscriber information is stored in the SM database and can then be distributed between multiple platforms according to actual subscriber placement.

The SM provides subscriber awareness, mapping network IDs to subscriber IDs. It obtains subscriber information using dedicated integration modules, which 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—On-demand, in response to a query from the SCE platform to the SM

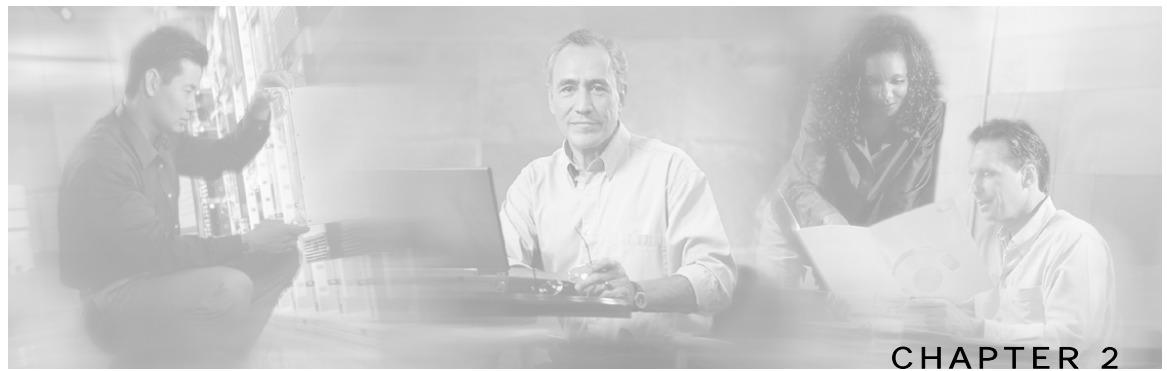
Service Configuration Management

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 & reporting, and control is created and applied to an SCE platform. *SCA BB* provides tools to automate the distribution of these configuration files to SCE platforms, and this simple, standards-based approach makes it easy to manage multiple devices in a large network.

Service Control provides an easy-to-use GUI to edit and create these files, as well as a complete set of APIs to automate their creation.

Collection

The Cisco Service Control solution generates usage data and statistics from the SCE platform and forwards them as Raw Data Records (RDRs), using a simple TCP-based protocol (RDR-Protocol). The Service Control solution provides the Cisco Service Control Management Suite (SCMS) Collection Manager (CM) software as an implementation of a collection system, listening in on RDRs from one or more SCE platforms, and processing them on the local machine. The data is then stored for analysis and reporting functions, as well as simple collection and presentation of data to additional OSS systems such as billing.



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, 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.

This chapter contains the following sections:

- [System Components](#) 2-1
- [Subscribers and Subscriber Modes](#) 2-3
- [Service Configuration](#) 2-5

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 complete information regarding the installation and operation of the SCE platform, see the *Cisco SCE Platform Installation and Configuration Guides*.

- The Cisco Service Control Management Suite (SCMS) Subscriber Manager (SM)—A middleware software component used in cases 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 (e.g. RADIUS, DHCP) and the SCE platforms

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

- The Cisco Service Control Management Suite (SCMS) Collection Manager (CM)—An implementation of a collection system, receiving 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 complete information regarding the installation and operation of the CM, see the *Cisco Service Control Management Suite Collection Manager User Guide*.

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

Together, the SCE platform, the SCMS-CM, the SCMS-SM, and the SCAS Reporter are designed to support detailed classification, analysis, reporting, and control of IP network traffic. Note that the SCMS-CM, the SCAS Reporter, and the SCMS-SM are optional components, and are not required in all deployments of the Cisco Service Control solution. 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 some or all of these components.

The following figure illustrates the flow of information within the Cisco Service Control solution.

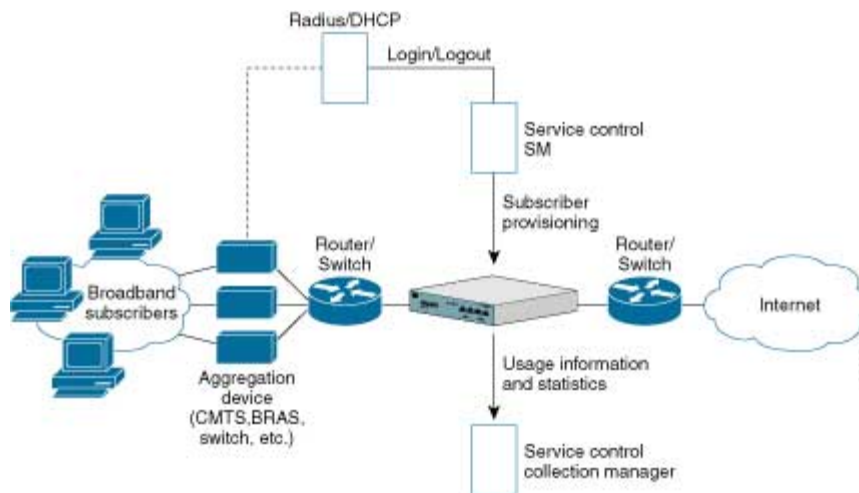
- Horizontal flow—Represents traffic between subscribers and IP network.

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 enables *SCA BB* to conduct subscriber level analysis and control.

Figure 2-1: Flow of Information in the Cisco Service Control Application for Broadband



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 that *SCA BB* can individually monitor, account and enforce a policy on. 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, it is also possible 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, as well as what actual policies to define. The following sections describe the different subscriber-modes supported, what functions are supported for each, what the prerequisites are, and which components are needed.

SCA BB supports the following four subscriber modes:

- Subscriberless mode—No subscribers are defined.
- 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 – dynamic subscribers—Subscriber information is dynamically bound to the IP address currently in use by the subscriber. This can be achieved through an integration with the system (Radius, DHCP) that assigns IP addresses to subscribers, or through sniffing this information. Policy information is either administered to *SCA BB* directly, or is also provisioned dynamically through 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, so the SCMS-SM is not required.



Note

Subscriberless mode is not influenced by the number of subscribers or inbound IP addresses, so that the total number of subscribers using the monitored link is unlimited from the perspective 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 no subscriber-differentiated control or subscriber-level quota tracking is required, when analysis on an IP level is sufficient, or when offline IP-address/subscriber binding can be performed. For example, it is possible to identify which subscribers generate the most P2P traffic by identifying the top IP addresses and correlating them to individual subscribers manually/offline via Radius/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 together incoming IP addresses into groups, so that traffic from and to defined subscribers can be controlled as a group. For example, with this mode, all traffic from and to a particular network subnet (used by multiple subscribers concurrently) can be defined 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, for example, a particular aggregation device, are to 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, and does not require external management software (for example, the SCMS-SM). This is achieved by using the SCE platform CLI to define the list of subscribers, their IP addresses, and the associated package.

Subscriber-Aware Mode: Dynamic Subscribers

In dynamic subscriber-aware mode, the Service-Engine is populated by subscriber information (OSS ID & policy) that is dynamically bound to the (IP) address currently in use by the subscribers. This provides differentiated and dynamic control per subscriber and subscriber-level analysis, regardless of the IP address in use. This mode is used to control and analyze traffic on a subscriber level and monitor subscriber usage, regardless of IP addresses. It also enables assigning and enforcing different control-policies (packages) for different subscribers.

In this mode the SCMS-SM may provision the SCE platform with subscriber information.

Subscriber Modes: Summary

The following table summarizes the different subscriber modes supported by the system.

Mode	Features Supported	Main Advantages	When to Use
Subscriberless mode	Global (platform-level) analysis & 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 mode	Global analysis & control Individual IP address level analysis & control	No subscriber-configuration required; only need to define subscriber IP address ranges used Provides 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 manually/offline with Radius/DHCP logs
Static subscriber mode	Global analysis & control Control based on individual IP addresses/groups as configured statically to the SCE platform	On-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
Dynamic subscriber mode	Full system functionality	Differentiated and dynamic control per subscriber Subscriber-level analysis, regardless of IP address in use	To control and analyze traffic on a subscriber level Monitor subscriber-usage, regardless of IP addresses Assign different control-policies (packages) to different subscribers, and change packages dynamically

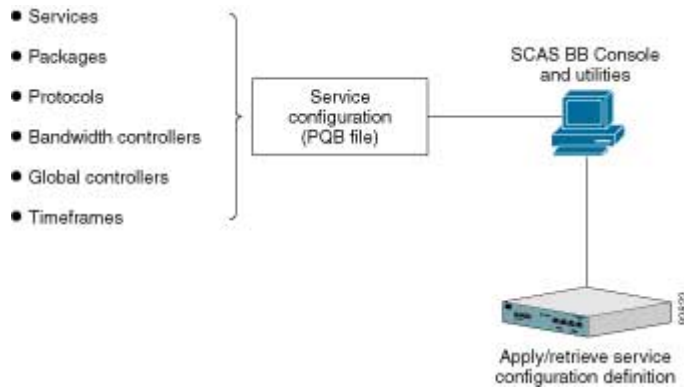
Service Configuration

Service configuration defines the way the SCE platform analyses and controls traffic. In very general terms, 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 SCAS BB Console
- The *SCA BB* Service Configuration Utility
- The Service Configuration API

The SCAS BB Console

The SCAS BB Console is a set of GUI tools that are used for management, configuration, and monitoring of the solution components.

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

The SCA BB Service Configuration Utility

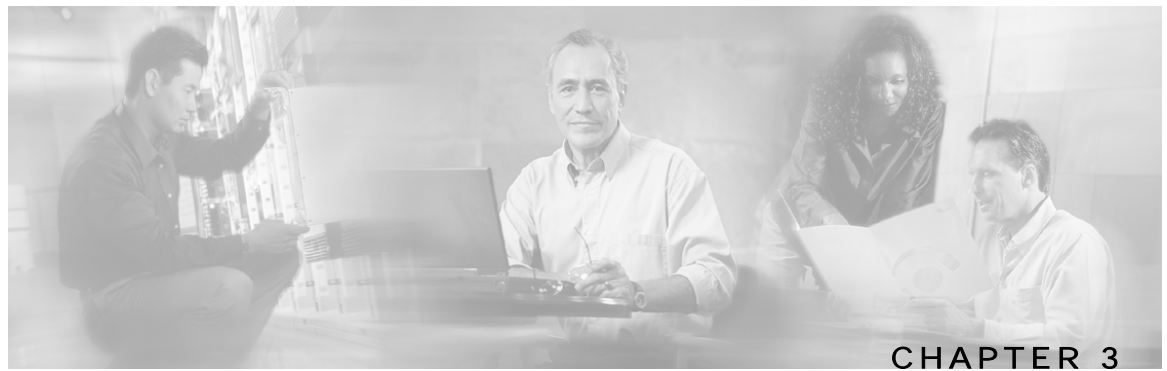
The *SCA BB* Service Configuration Utility (`servconf`) is a simple command-line utility that can be used to apply PQB configuration files onto SCE platforms, or retrieve the current configuration from an SCE platform and save it as a PQB file. The tool can be installed and executed in a Windows or Solaris environment, and configures SCE platforms with the service configuration defined in a PQB file.

See *The Cisco Service Control Application for Broadband Service Configuration Utility* (on page 13-1) for full documentation of `servconf`.

Service Configuration API

The Service Configuration API is a set of Java classes used to program and manage service configurations, and to apply these service configurations to the SCE platforms. In addition, applications using the Service Configuration API can be integrated with third-party systems, allowing service providers to automate and simplify management and operational tasks.

The Service Configuration API is documented in the *Cisco SCA BB Service Configuration API Programmer's Guide*.



Traffic Processing Overview

This chapter describes how traffic is processed by the *Cisco Service Control Application for Broadband (SCA BB)* when it flows through a Service Control Engine (SCE) platform with *SCA BB* installed.

The chapter gives an overview of the three stages of traffic processing:

- **Traffic Classification**—*SCA BB* analyses traffic flows and determine their type (for example, browsing, email, file-sharing, voice and so on)
- **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* can be set to limit and prioritize traffic flows according to service, subscriber-package, subscriber quota state, and so on

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

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

This chapter contains the following sections:

- [Traffic Classification](#) 3-1
- [Traffic Accounting and Reporting](#) 3-7
- [Traffic Control](#) 3-10
- [Other Traffic Processing Features](#) 3-16
- [Service Configurations](#) 3-16

Traffic Classification

Traffic processing starts with *traffic classification*. The classification process categorizes network sessions into services. Services are the entities which are:

- The building blocks for service configuration, as different rules can be enforced on different services
- The building blocks for aggregated usage reporting

For each commercial service that a provider offers to its subscribers, a corresponding service is defined in the Cisco Service Control solution. This service is used to classify and identify the traffic, report on its usage, and control it, as required.

Services

SCA BB performs the classification process, which categorizes network sessions into *services*.

Services are:

- The building blocks for service configuration, because different policies can be enforced on different services
- The building blocks for aggregated usage reporting

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 the service configuration.

There can be a maximum of 500 services in a service configuration.

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; this ID does not change during the session's life-cycle.

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

- Protocol—Using the SCE platform deep-packet-inspection capability, the system classifies network traffic according to the protocol used. This allows, for example, the mapping of browsing flows and email flows to separate services.
- Initiating side—Flows can be classified to different services according to whether the flow was generated by the subscriber-side or the network-side. This allows, for example, the mapping of subscriber-initiated and network-initiated peer-to-peer traffic to separate services.
- Zone—Lists of network-side IP addresses: 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: for instance, 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.

From a provider's perspective, a service is a network product sold to a subscriber; a service is usually a network application, such as browsing, email, file-sharing or voice, which the subscriber is using. From a technical perspective, a service consists of one or more service elements, each element enabling a decision regarding the service associated with a network traffic flow type.

These flow mappings are used by **SCA BB** to map each network connection passing through it to a service. Rules can then be applied to the different services to implement control policies. The classification rules can contain L3 and L4 parameters (such as port numbers and IP addresses), as well as L7 parameters (such as host name and user agent for HTTP connections).

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.

A service is a collection of service elements.

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 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



Note

If a flow matches two service elements:

If one service element is more specific than the other, the flow will be mapped to the more specific service element.

For example: Service A - browsing, Service B - 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, which is more specific.

If the 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 - email, Service B - all traffic to a specific network zone; an email flow to the specific network zone matches both services, but will be mapped to Service A, because protocols have higher precedence than zones.

Examples of Services

The following table 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

The *protocol* of a session (rather, the network application that generated the session) is one of the main ways of classifying a flow.

The protocol of the flow is determined by its signature, port number, and transport type. 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 following points summarize the main aspects of protocols in the *SCA BB* system:

- A protocol, as defined in the system, is a combination of one or more signatures, one or more port numbers, and a transport type.
- The protocol of the network flow is identified according to these parameters.
- The default service configuration contains a long list of predefined protocols. Additional protocols can be added by the user.
- 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.

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 protocol is a collection of protocol elements.

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



Note

If a flow matches two protocol elements:

If one protocol element is more specific than the other, the flow will be mapped to the more specific protocol element.

For example, Protocol A - flows that match the FTP signature, Protocol B - 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 which is more specific.

If the 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 - flows that match the FTP signature, Protocol B - flows on TCP port 21; an FTP flow on port 21 matches both protocols, but will be mapped to A, because signatures have higher precedence than port numbers.

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, email, file-sharing, and voice.

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 user-defined signatures, *Dynamic Signatures*.

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 as well as the predefined signatures.

Initiating Side

The SCE platform is usually located between the provider's subscribers and the network. Subscriber-initiated flows are those initiated by the subscriber toward the network, while network-initiated flows are those initiated from the network toward the subscriber.

Certain types of flows can be limited to one initiating side. For example, with HTTP it is possible to restrict the direction of the flow to subscriber-initiated, since 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 has been opened 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.

Zones are configured by the user; IP addresses are arranged in groups connected by a common purpose and on which a subscriber's network flow mapped to a service may be applied. 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 range 10.2.0.0/16. Analysis of a new session shows that its network IP address is 10.1.1.1; consequently the session's zone is zone A.

Zone Item

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

A zone is a collection of related zone items.

Table 3-2 Examples of Zone Items

Network Address	Example
IP address	123.123.3.2
IP address range (and mask)	A range of IP addresses including mask can be of the form 123.3.123.0/24. This means that the first 24 bits of the IP address should be included as specified, and the remaining 8 bits or 256 IP addresses included in the range.

Flavors

Flavors are advanced classification elements that are used to classify network sessions according to signature-specific L7 properties.

Protocol 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.

Flavor types include, for example, HTTP URL, HTTP User Agent, and SIP Domain.

Flavor Item

A flavor (such as HTTP Streaming) is a list of *flavor items* (such as names of HTTP user agents). The type of these flavor items depend on the flavor type.

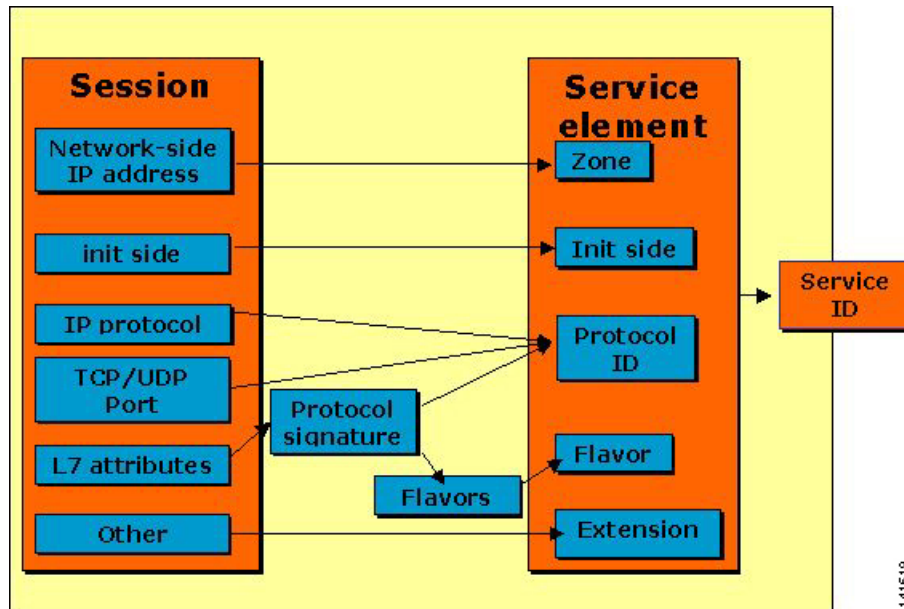
See *Flavor Types and Parameters* (on page 7-48) for a list of available flavor types.

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

Mapping Flow Attributes to Services

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

Figure 3-1: Mapping Flow Attributes to Service



Traffic Accounting and Reporting

Data gathered by the SCE platforms can be used 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 counters.

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

- Raw Data Records (RDRs) can be generated containing flow, usage, and other data. These RDRs are transmitted by the SCE platform.
- The SCE platform maintains an SNMP MIB. This 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 Kbytes)
- Downstream volume (L3 Kbytes)
- Sessions
- Active subscribers

- Concurrent sessions
- Session duration

**Note**

For voice services, such as SIP and MGCP, the concurrent sessions counter measures concurrent voice calls, and the session duration counter measures voice call duration

Per service accounting takes place in the following scopes:

- Per subscriber
- Per group of subscribers (package)
- Per the entire link

Several services may share the same counter. For example, in the default service configuration, the SMTP service and the POP3 service share a single Email service counter. The assignment of services to counters is determined by service hierarchy, as explained in the following section. Similarly, packages may share the same counter, and the assignment of packages to counters is determined by package hierarchy (see *The Package Hierarchy* (on page 3-9)).

The Service Hierarchy

Services are arranged in a hierarchal tree. A single Default Service is at the root, and each new service can be placed anywhere in the tree.

Services inherit the rule of their ancestors. 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 Counters

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

There are two categories of usage counters for services:

- Global—Used for Link and Package RDRs & reports
- Subscriber—Used for Subscriber RDRs & reports

A global counter and a subscriber counter are assigned to each service. The use of a service can either be accounted exclusively for traffic classified to it, or in conjunction with the traffic of its parent service. For example, if a service “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 counter as “Streaming”. The global counter and the subscriber counter are independent; in other words, for the same service, one counter may be the same as the parent service, while the other is exclusive to the child.

The Package Hierarchy

Packages are arranged in a hierarchical tree. A single Default Package is the root of the tree, and each new package can be placed anywhere in the tree.

Package Counters

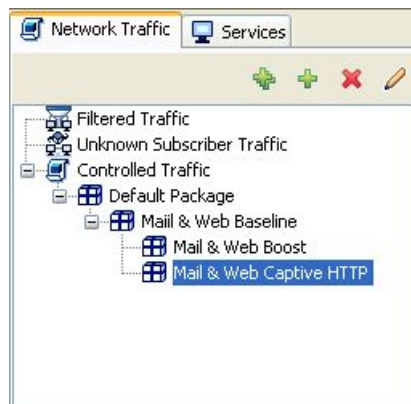
The package hierarchy provides a way to share package usage counters, as well as to organize packages according to their semantics. A maximum of 64 different exclusive package counters can be defined, one of which is defined for the Unknown Subscriber Traffic package.

Usage reporting at a package level is grouped as follows:

- Package assigned an exclusive package 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 counter—All traffic associated with this package is accounted together with its parent package.

For example, in the sample package hierarchy shown in the following figure, if the Mail & Web Baseline package is allocated an exclusive counter, but none of its child packages are, then all Package Usage RDRs and the derived reports (such as “Package Bandwidth per Service”) would group together usage of subscribers assigned to all three packages.

On the other hand, if, say 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, while traffic for Mail & Web Boost would be accounted separately. (This is instructive as an example, but in general is not efficient as an actual configuration because the hierarchical structure should be used to group packages that can use the same counter.)



RDRs

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

RDRs contain a wide variety of information and statistics, depending on the configuration of the system. The following are the main categories of RDRs:

- Usage RDRs—Records generated periodically that contain the state of the usage counters, per service and per accounting scope, as follows:
 - 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 and used by the Cisco Service Control Management Suite (SCMS) Collection Manager (CM) and Cisco Service Control Application Suite (SCAS) Reporter for top-subscriber reports and to generate aggregated usage billing records
- Real-Time Subscriber Usage RDRs—Generated for specific subscribers selected by the user, these RDRs are used by the SCMS-CM and SCAS Reporter to generate detailed subscriber activity reports
- Flow RDRs—Records generated for a sample of the flows, used to create statistical histograms such as Top TCP Ports
- Flow Usage RDRs—Generated for every flow according to user defined filters, these RDRs contain detailed L7 information for browsing, streaming, and voice flows and can be used for flow-based billing
- Real-time signaling RDRs—Generated to indicate specific network events such as flow start or end, these RDRs can be 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

Traffic Control

Traffic Control provides the more advanced functionality of the Cisco Service Control solution.

Packages

A *package* defines the group of services delivered to a specific group of subscribers; it is a description of subscriber policy. It contains the definitions of the system's behavior per service, such as any restrictions on network flows, guidelines for the flow's prioritization, or instructions regarding how the flow should be reported; a package is a collection of rules.

Each subscriber in the network is provided a reference to a package to which that subscriber belongs. The system maps the network flow to a certain service if it fits the definition of one of its service elements. In addition, the system identifies the subscriber to whom the flow pertains, according to the subscriber's network ID (usually the subscriber's IP address). Thus, the package the subscriber belongs to can be determined, and the correct rule can be applied to the service of the subscriber's network flow.

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 that is 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 to the SCE platform telling it how to treat network flows of a specific service. A rule may specify that a flow should be blocked, or granted a certain amount of bandwidth. It may also define an aggregate volume or session limit, after which a set of different restrictions may be enforced on the flow. A rule may also specify how a flow should be reported for billing or analysis purposes.

Time-Based Rules

SCA BB allows you to split the week into four *time frames*. 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, the rules for the different time frames will 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 then make any needed changes. Subsequent changes to the parent rule do not affect the time-based rule.

Calendars

Calendars are used to split the hours of the week into four time frames.

Once you have configured a calendar, you can add time-based rules to a package that is using 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 only apply 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. In addition, you can add another nine calendars, each with a different time-frame configuration. Different calendars can be used for different packages. They can also be used where a service provider has customers in more than one time zone.

Bandwidth Management

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

- Global control
- Subscriber bandwidth control

Link Bandwidth Limit

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 less than the link limit.

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.

Global Bandwidth Control

Total bandwidth use is controlled by *global controllers*. Global controllers are virtual queues in SCE platforms. They are configured for the entire system, rather than for individual subscribers.

The purpose of the global controllers is to provide constraints for large, global volumes of traffic, such as "Total Gold Subscriber Traffic", or "Total P2P Traffic". Each global controller defines the percentage of total available bandwidth allocated to all traffic of a particular type or types. 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, keeping 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% of the link traffic. You can add up to 63 more global controllers for each interface, and assign a maximum percentage of the total link limit to each global controller separately.

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:

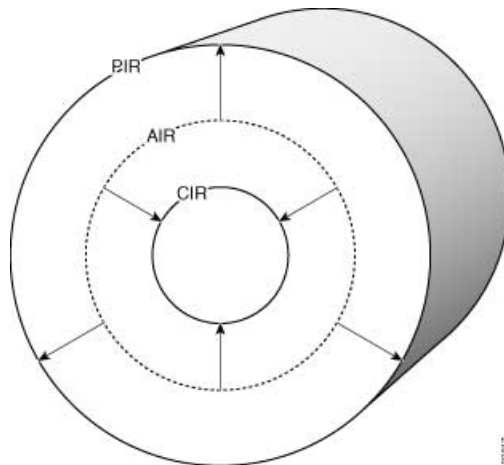
- Committed Information Rate (CIR)—The minimum bandwidth that must be granted to the services that are controlled by the BWC
- Peak Information Rate (PIR)—The maximum bandwidth that will be allocated to the services that are controlled by the BWC
- Global Controller—The global controller to which this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

PIR can be thought of as the "width" of the virtual pipe; assume that the pipe is flexible and may adjust in width. CIR is the minimum width to which the pipe can contract. During network congestion, the system contracts each pipe differently to differentiate between subscribers and between their services.

The pipe width in this analogy defines the total bandwidth (Admitted Information Rate (AIR)) that is allowed to cross the pipe; AIR ranges between CIR and PIR. The consumed bandwidth (UIR) is the rate that currently flows through the BWC and it is always less than AIR.

It might be that the traffic associated with the BWC does not consume much bandwidth at a particular point in time. However, in case there is a growing demand for bandwidth, the BWC ensures that at least the CIR is granted, even in conditions of network congestion (PIR-congestion). Similarly, the BWC ensures that no matter of congestion conditions, the traffic associated with a BWC would always be below the PIR limit.

Figure 3-2: Bandwidth Control Levels



In the preceding figure, the small circle indicates CIR. The big circle indicates PIR. The dashed circle indicates AIR - the maximum rate currently allowed to flow through the BWC: $CIR < AIR < PIR$. UIR - the rate that currently flows through the BWC - can be smaller than CIR: $0 < UIR < AIR$.

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

Controlling Traffic at Two Levels: Total and Internal

Subscriber BWCs enforce bandwidth at two levels:

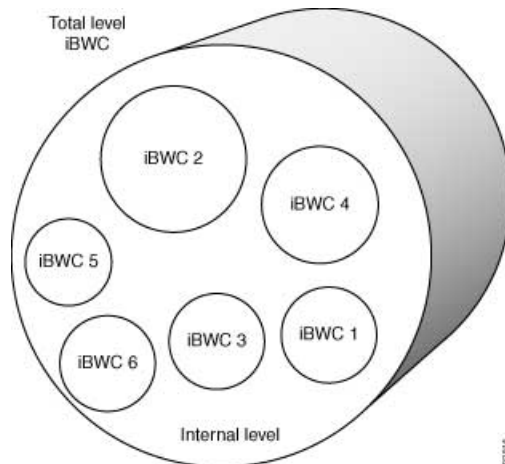
- The first level, Primary (Total) BWC, specifies bandwidth service configurations that the *provider* enforces on its subscribers
- The second level, (Internal) BWC, specifies service configurations that the *subscriber* wants to enforce on its services

SCA BB provides each subscriber with an independent set of BWCs. A single BWC is used to control the total bandwidth of the subscriber. This BWC, which provides the first-level control, is referred as the Primary BWC (tBWC).

The other BWCs control the bandwidth of some services of that subscriber. For example, one BWC may control the Streaming Service, while another may control the Download and E-mail Services together. These BWCs, which provide second-level control, are referred as iBWCs.

PIR defines the upper limit for the associated services. CIR defines a minimum rate for these services. The system ensures that this minimum is granted under conditions that will be described later.

Figure 3-3: Bandwidth Control on Two Levels



The primary BWC (tBWC) controls the total bandwidth of the subscriber. iBWCs control the bandwidth of portions of this bandwidth that are associated with one or more services.

iBWCs are linked to traffic in the following way:

- In the package general definitions, define a BWC, with its PIR, CIR, AL and CoS
- When defining a rule, assign each service to one BWC

Quota Management

Subscribers can be assigned a quota limit on selected services.

Each subscriber has 16 quota buckets, and each bucket can be defined 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. In the case of volume buckets, consumption is counted in units of L3 kilobytes. In the case of session buckets, consumption is the number of sessions. For example, it is possible to define that the Browsing and E-Mail services consume quota from Bucket #1, 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, it is possible to increase the quota of a certain bucket when a subscriber purchases additional quota. These systems can also query the amount of remaining quota in each bucket. This can be used, for example, to show subscribers (for example, in a personal web page) how much of their quota remains.

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

Optionally, subscribers can be notified when they breach the quota in any bucket.

Subscriber Notification

The subscriber notification feature provides the means to push 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.

Other Traffic Processing Features

Traffic Filters

Filter rules are part of the service configuration. 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 transmit the flows unchanged.

When a traffic flow enters the SCE platform, the platform checks whether a filter rule applies to this flow.

If a filter rule does apply 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 within any records generated for analysis purposes nor will the flows 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) which might traverse the SCE platform - these protocols usually should not be affected by policy enforcement; also they are of low volume, and insignificant for reporting.

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

Traffic Forwarding to VAS Servers

Traffic forwarding to Value Added Services (VAS) servers allows the Cisco Service Control solution to use an external expert system for additional traffic processing. When using this feature, traffic is rerouted by the SCE to the pre-configured location of the expert system (VAS server). After processing, the traffic is sent back to the SCE which then sends it to its original destination. Conceptually, this feature adds one additional step (the expert system redirection) to the traffic processing done by *SCA BB*.

Service Configurations

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

Before a service configuration takes effect, it needs to be 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**—A service configuration contains services, such as Web Browsing, File Sharing, and Voice. Each service consists of service elements; the service elements define which network traffic is mapped to the service. Protocols, zones, flavors and signatures are the configuration building blocks of services.
- **Traffic Accounting and Reporting Settings**—A service configuration contains settings that determine how traffic flows and network usage accounting are reported.

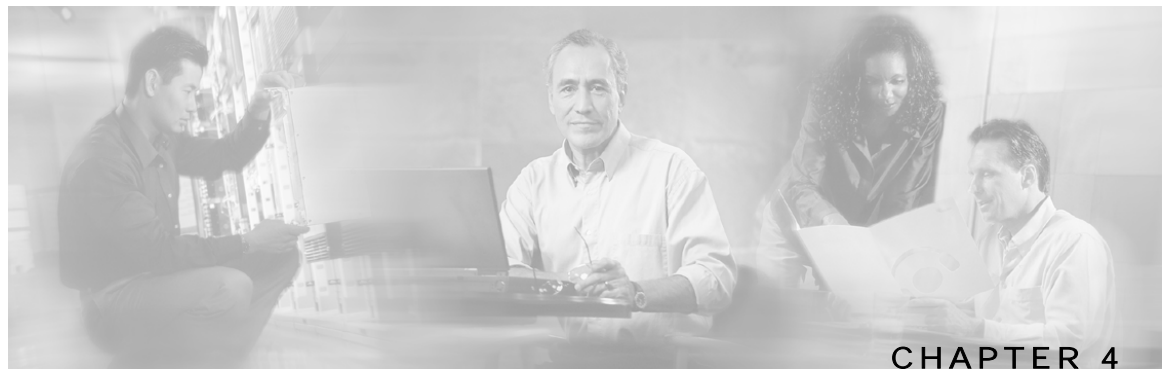
- **Traffic Control Settings**—A service configuration contains packages, each package consisting of a set of rules (such as bandwidth rate limit and quota limits) defined for different services. Rules, quota buckets, subscriber BWCs, and global controllers are the main configuration building blocks of traffic control settings.

Defining Service Configurations in Practice

In practice, defining service configurations is an iterative process.

It is recommended that you:

- Set up the system
- Apply the default service configuration
- Gather data
- Analyze
- Only then, decide what you want to do:
 - Continue traffic discovery by further partitioning the traffic into services
 - Achieve capacity-control and tiered-control goals by creating rules to limit and prioritize traffic according to services and subscriber packages



Getting Started

This chapter:

- Guides you through the process of installing or upgrading the *Cisco Service Control Application for Broadband (SCA BB)*
- Explains how to launch the various components of the SCAS BB Console
- Describes the notion of the SCAS BB Console as a collection of tools, presents each tool and its role, and describes how to navigate between the tools
- Concludes with a Quick Start section that describes how to apply your first service configuration and generate your first report

This chapter contains the following sections:

- [Installing SCA BB 4-1](#)
- [Upgrading from Version 2.5 to Version 3.0 4-13](#)
- [Launching the SCAS BB Console 4-14](#)
- [Using the SCAS BB Console 4-16](#)
- [Quick Start with the SCAS BB Console 4-23](#)

Installing SCA BB

Installation of *SCA BB* is performed in two stages:

Step 1 Installation of the *SCA BB* application components:

- The *SCA BB* Service Control Engine (SCE) applicative management plug-in
- The *SCA BB* Subscriber Manager applicative management plug-in (for systems where a Cisco Service Control Management Suite (SCMS) Subscriber Manager (SM) is present)

Step 2 Installation of the *SCA BB* front ends:

- The SCAS BB Console
- The *SCA BB* Service Configuration Utility and the *SCA BB* Signature Configuration Utility

If you are upgrading an existing installation of **SCA BB**, see *Upgrading from Version 2.5 to Version 3.0* (on page 4-13).

Prerequisites

Before installing **SCA BB**, verify that the Service Control Engine (SCE) platform and, if used, the SCMS-SM are operational and running appropriate versions of their software.

To verify that the SCE platform is operational:

Verify that the status LED on the SCE flashes green. (Other colors indicate booting up (orange), warning (flashing orange) or failure (red).)

To verify that the SCE platform is running an appropriate version of the OS:

At the SCE platform CLI prompt (SCE#) type:

show version and press **Enter**

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

To verify that the SM is correctly installed:

Open a Telnet session to the SM, and then go to the SM `bin` directory and type:

```
> p3sm --sm-status
```

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

To verify that an appropriate version of the SM is running:

Open a Telnet session to the SM, and then go to the SM `bin` directory and type:

```
> p3sm --sm-version
```

The response to this command displays the SM version.

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:

- *scas-bb-console-3.0.0-<build>.exe*—The installer for the SCAS BB Console
- 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
- *scas_bb_util.tgz*—Contains the files for *servconf*, the *SCA BB* Service Configuration Utility, and *sigconf*, the *SCA BB* Signature Configuration Utility
- *PCubeEngageMib.mib*—Defines the *SCA BB* BB MIB
- *serviceconfig-java-api-dist.tgz*—The *SCA BB* Service Configuration Java API distribution file

Installing SCA BB Application Components

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

- The *SCA BB* SLI—The application 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

These components are installed by uploading an appropriate PQI file to the SCE platform or to the SM device.

Installing a SCA BB PQI File on an SCE Platform



Note After you install the SCAS BB Console, you can install a PQI file on an SCE using the Network Navigator tool (see *Installing PQI Files on SCE Devices* (on page 5-12)).

To install a *SCA BB* PQI file on an SCE platform:

Step 1 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 In the command line of the SCE platform, type:

```
>enable 10
Password: *****
#configure
(config)#interface LineCard 0
(config if)#pqi install file engXXXXXX.pqi
```

Step 3 Monitor the installation progress until it is completed.

The PQI file is now installed.

Installing a SCA BB PQI File on an SM Device

If the system configuration includes an SCMS-SM, install the SM PQI.



Note After you install the SCAS BB Console, you can install a PQI file on an SM device using the Network Navigator tool (see *Installing PQI Files on SM Devices* (on page 5-17)).

To install a *SCA BB* PQI file on an SM device:

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_engXXXXXX.pqi
```

Step 4 Monitor the installation progress until it is completed.

The PQI file is now installed.

Installing SCA BB Front Ends

The following *SCA BB* front ends should be installed:

- The SCAS BB Console is installed with a single process (wizard) (see *Installing the SCAS BB Console* (on page 4-5))
- The *SCA BB* Service Configuration Utility (*servconf*) and the *SCA BB* Signature Configuration Utility (*sigconf*) (see *Installing the SCA BB Configuration Utilities* (on page 4-8))

System Requirements

- The *SCA BB* GUI front ends can be installed on any computer running Windows 2000, Windows XP, or Windows Server 2003.
- Internet Explorer version 5.5 or higher is required.
- The computer should have a minimum of 256 MB of memory.
- To run *servconf*, the *SCA BB* Service Configuration Utility, a Java Runtime Environment must be installed on the workstation

Installing the SCAS BB Console

To install the SCAS BB Console:

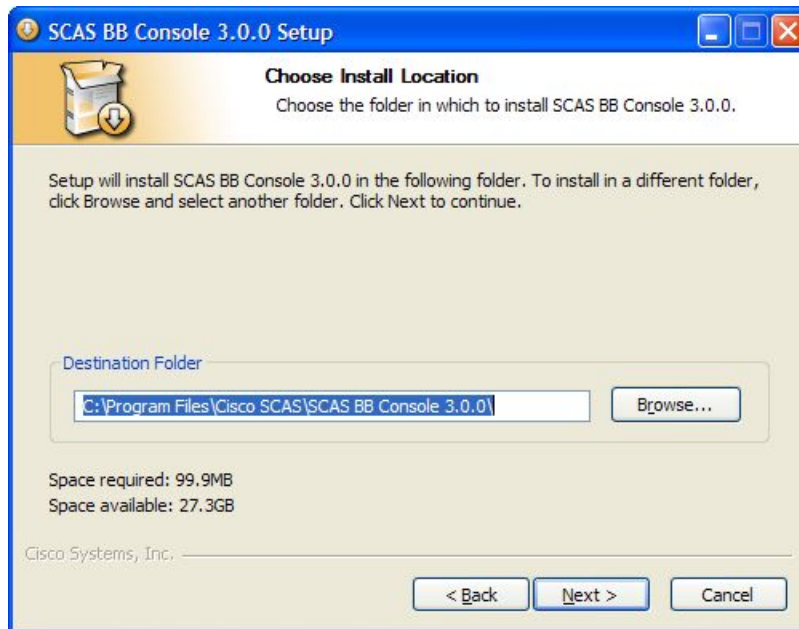
- Step 1** Navigate to the SCAS BB Console installation file, *scas-bb-console-3.0.0.exe*, and double-click on it.

The SCAS BB Console 3.0.0 Setup Wizard Welcome screen appears.



- Step 2** Click Next.

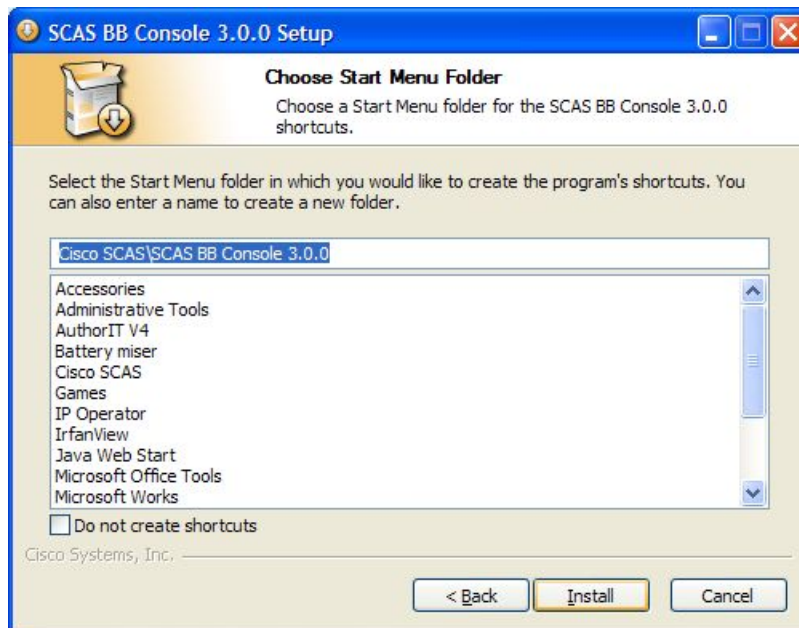
The Setup Wizard Install Location screen appears.



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

Step 4 Click **Next**.

The Setup Wizard Start Menu Folder Screen appears.

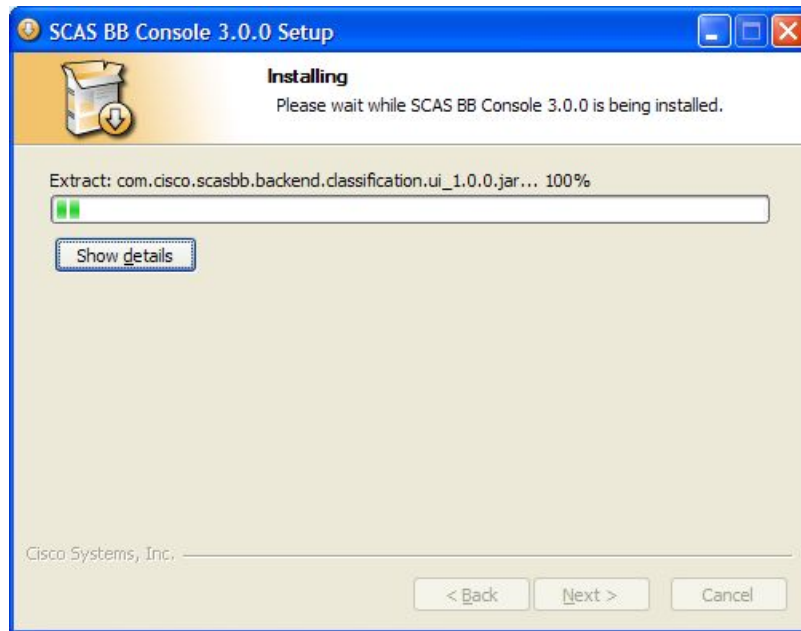


Step 5 (Optional) Enter a different Start Menu folder in the Start Menu Folder field.

Step 6 (Optional) Check the Do not create shortcuts checkbox.

Step 7 Click **Install**.

The Setup Wizard Installing screen appears.

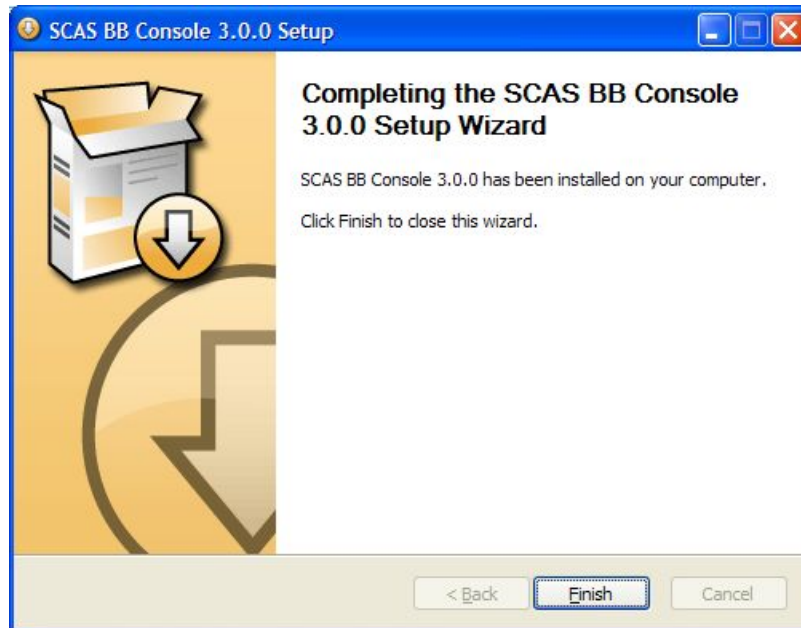


Step 8 Wait until installation is complete.

The Next button is enabled.

Step 9 Click Next.

The Setup Wizard Complete screen appears.



Step 10 Click Finish.

The SCAS BB Console 3.0.0 Setup Wizard closes

The SCAS BB Console is now installed on the machine.

Installing the SCA BB Configuration Utilities

To install the *SCA BB* Configuration Utilities:

Step 1 Locate 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*, and the *SCA BB* Signature Configuration Utility, *sigconf*, are located under the *bin/* folder.

Installing the Java Runtime Environment

servconf requires Java Runtime Environment (JRE) version 1.4 or 1.5.

The JRE can be downloaded 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, 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
```

Installing 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 L3 to L7 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. A protocol support plug-in can be loaded 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 down-time.

Protocol Packs

Cisco publishes protocol packs periodically. These packs include 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 interesting protocols. When loaded into SCE platforms, these signatures improve *SCA BB* classification abilities.

A protocol pack for *SCA BB* can be of one of two types: an SPQI file or a DSS file.

**Note**

A protocol pack can only be installed on an SCE platform if a PQI is already installed on the platform.

DSS Files

DSS files contain new and improved signatures for *SCA BB*. Loading a DSS file to the SCE platform requires no downtime of *SCA BB* or the platform.

SPQI Files

Like DSS files, SPQI files contain new and improved signatures for *SCA BB*. Unlike DSS files, loading an SPQI file to the SCE platform entails updating the SCE application; this is necessary when a fundamental signature update is required.

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.

Updating Protocols

Verifying Version Compatibility for Protocol Packs

A protocol pack is compatible only with specific versions of the SCE application. When working with protocol packs, it is important to verify that the protocol pack version matches the SCE application version. For example, a protocol pack for 3.0.0 should only be used on SCE application version 3.0.0.

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

To verify that the protocol pack can be successfully installed:

-
- Make sure that the correct version of *servconf* is installed and running correctly:

- From the command prompt, run **servconf --version**

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

- Make sure that the correct version of the SCE application is installed:

- At the SCE platform CLI prompt (SCE#) type:

show version and press **Enter**

The application version should match that of the protocol pack.

- Make sure a service configuration (PQB) is applied to the SCE platform:
 - In the SCAS BB Console, retrieve and view the current PQB
-

Distributing Protocol Packs

Installing a protocol pack on an SCE platform is performed using the Network Navigator tool (described in the following section) or the `servconf` command-line utility (see *The Cisco Service Control Application for Broadband Service Configuration Utility* (on page 13-1)).

The tool or utility performs the following steps:

- Step 1** Retrieves the current service configuration from the SCE platform and (optionally) store a backup copy in a user-specified folder.
- Step 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.
- Step 3** Adds new signatures to appropriate services.

For each new signature that includes a Buddy Protocol attribute (an attribute that points to an existing protocol): adds the new signature to all services where the buddy protocol appears (see *The Buddy Protocol* (on page 12-3)).
- Step 4** If the protocol pack is an SPQI file—Replaces the SCE application. This causes a short (up to one minute) SCE platform service downtime.
- Step 5** Applies the new service configuration to the SCE platform.

Installing a Protocol Pack

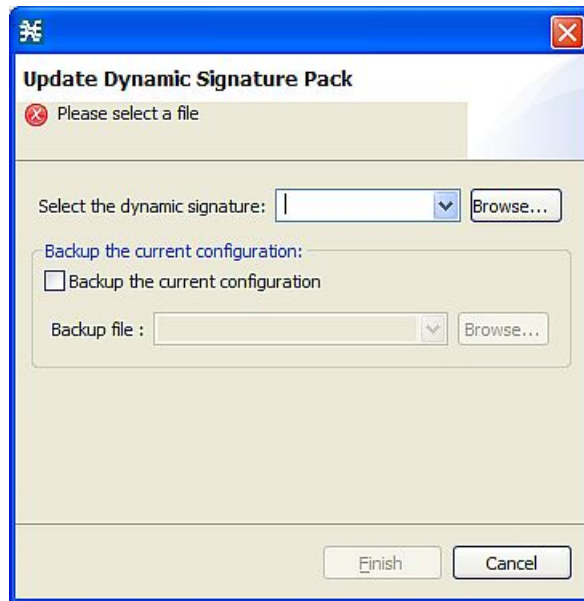
The Network Navigator allows easy installation of protocol packs.

You can install protocol packs on a single SCE platform, on selected SCE platforms, or on all SCE platforms at one or more selected sites.

To install a protocol pack on a single SCE platform:

- Step 1** In the Site Manager tree, right-click on the SCE where the protocol pack is to be installed and, from the short-cut menu, select **Update Dynamic Signature Pack**.

The Update Dynamic Signature Pack dialog box appears.



Step 2 Click **Browse**.

A Select file dialog box appears.

Step 3 From the Files of type drop-down list, select ***.spqi** or ***.dss**, as appropriate.

Step 4 Browse to the file to be installed.

Step 5 Click **Open**.

The Select file dialog box closes.

The Finish button is enabled.

Step 6 (Optional) Check the Backup the current configuration check box, and select a backup file.

Step 7 Click **Finish**.

A Password Management dialog box appears.

Step 8 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

Step 9 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.

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 is to be installed, right-click on one of them, and, from the short-cut menu that appears, select **Update Dynamic Signature Pack**.

The Update Dynamic Signature Pack dialog box appears.

- Step 2** Select the protocol pack to be installed and click **Finish**.

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 **Update**.

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

Verifying the Installation of a Protocol Pack

To verify that the protocol pack was installed successfully:

- Step 1** At the SCE platform CLI prompt (SCE#) type:

show version and press **Enter**

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

- Step 2** Retrieve the PQB from the SCE platform and view it using the SCAS BB Console. You should be able to see that the new protocols from the protocol pack were added to the service configuration.

Troubleshooting the Protocol Pack Installation

Any of the following may cause the installation of a protocol pack to fail:

- Missing or incorrect version of the JRE—See *Installing the Java Runtime Environment* (on page 4-8)
- Incorrect or missing SCE application version on the SCE platform—Validate the correct SCE application is installed as explained above.
- No service configuration (PQB) is applied to the SCE platform—Create a new PQB and apply it using the SCAS BB Console
- *servconf* failed to import the new signatures into the PQB—Use the **--force-signature** update signature option when running *servconf*

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

Upgrading from Version 2.5 to Version 3.0

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

- The SCAS BB Console
- The *SCA BB* SCE applicative management plug-in (SCE PQI file)
- The *SCA BB* SM applicative management plug-in (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.

To upgrade *SCA BB* application components:

- 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
- Step 2** Install the SCAS BB 3.0 Console (see *Installing the SCAS BB Console* (on page 4-5))
- Step 3** Open the SCAS BB 3.0 Console
 - a) Use the Network Navigator tool to install a version 3.0 SCE PQI file on the SCE platform
 - b) Verify that the installation was successful by retrieving the online status from the SCE platform using the Network Navigator
- Step 4** If your system includes an SM, use the Network Navigator tool to install a version 3.0 SM PQI file on the SM device

- Step 5** Open the service configuration saved in step 1 with the 3.0 Service Configuration Editor tool
- Step 6** When upgrading old PQB files, new signature-based protocols are not assigned to any service. Signature-based protocols that are not assigned to a service are classified as Generic TCP. To fix this, manually assign these protocols to a service. Check the release notes for a list of new signature-based protocols.
- Step 7** Apply the service configuration to the SCE platform
-



- Note**
- When upgrading 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** versions do not use the default DSS that was installed for a previous **SCA BB** version (see *The Default DSS File* (on page 7-37))
 - If a protocol pack for the new version is available, it should be installed once the product installation is complete (see *Installing a Protocol Pack* (on page 4-10)); do *not* install an old protocol pack on top of a new product installation
-

Upgrading the SCA BB Service Configuration Utility

Install the new version of the **SCA BB** Service Configuration Utility, *servconf*, in an empty directory (see *Installing the SCA BB Configuration Utilities* (on page 4-8)).

Launching the SCAS BB Console

The SCAS BB Console installation wizard adds a shortcut to the start menu for the SCAS BB Console.

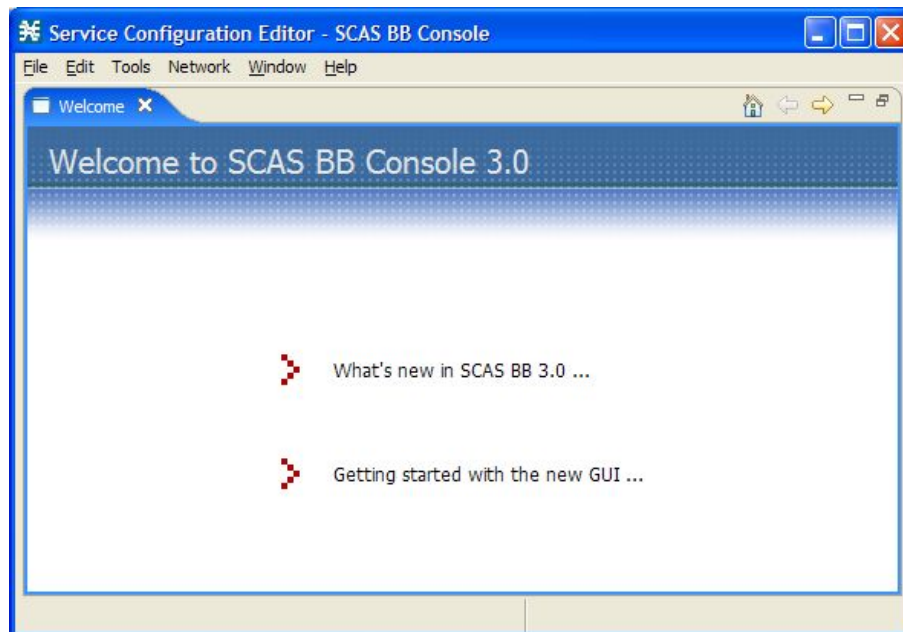
To launch the SCAS BB Console:

- Step 1** Choose **start > All Programs > Cisco SCAS > SCAS BB Console 3.0.0 > SCAS BB Console 3.0.0**

The Cisco Service Control SCAS BB Console splash screen appears.

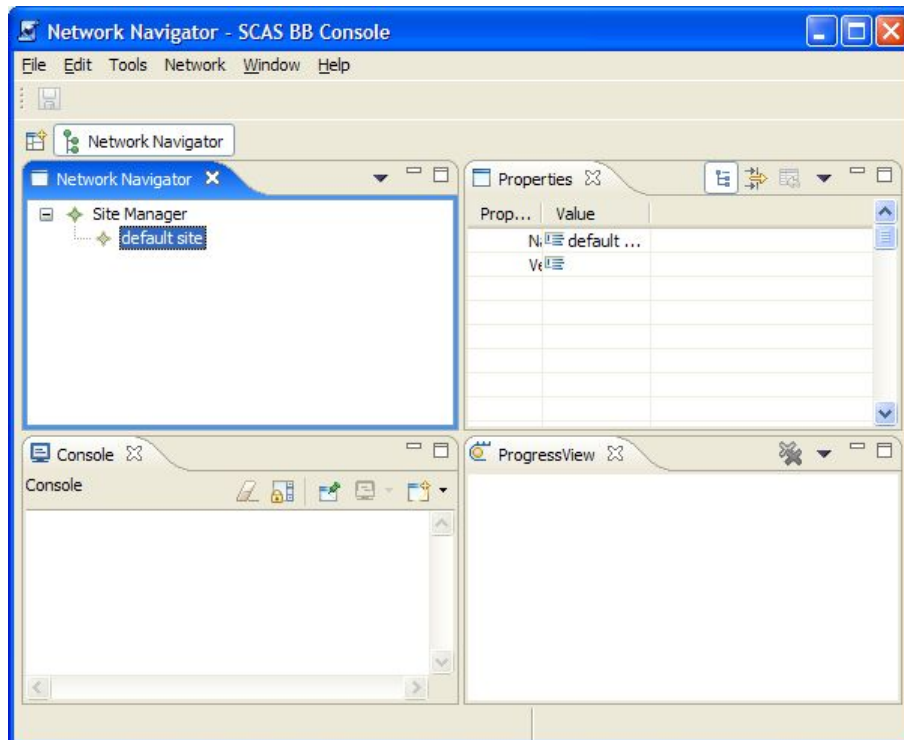


Once the console has loaded, the SCAS BB Console window opens, displaying the Welcome tab.



Step 2 Close the Welcome tab.

The main window of the SCAS BB Console appears, with the Network Navigator tool open.



Using the SCAS BB Console

The SCAS BB Console is the front end of the *Cisco Service Control Application for Broadband*. It is used to configure the services that the SP offers its clients.

Navigating in the SCAS BB Console

The SCAS BB Console is a collection of tools. These tools are introduced in the following sections.

The SCAS BB Console GUI has a menu bar and a standard toolbar. Underneath the toolbar is another bar that displays buttons of any SCAS BB Console tools that are open. When you launch a tool, a button is added to this bar. To switch between open tools, simply click on the appropriate button on the bar.



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

The Network Navigator Tool

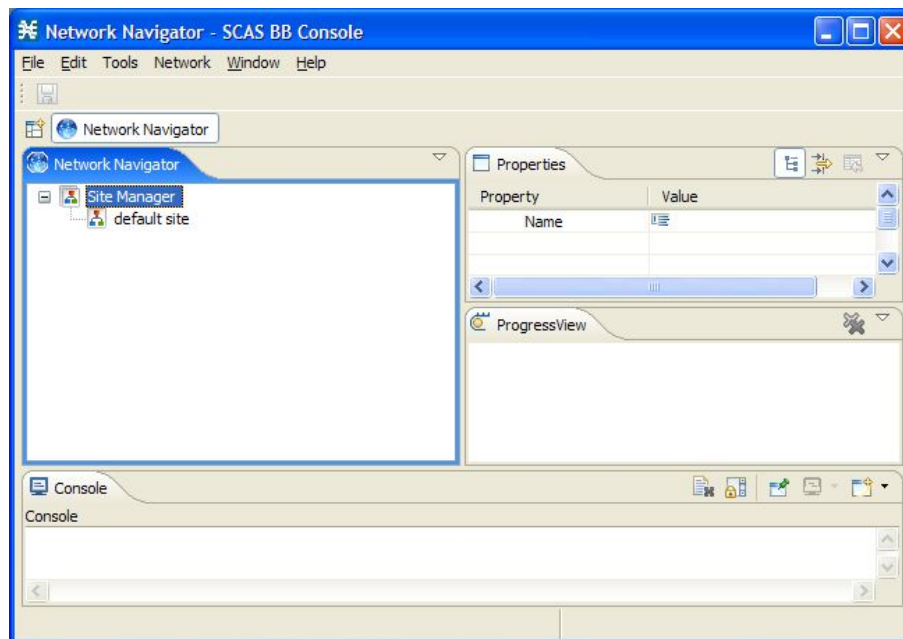
The Network Navigator is a tool that allows you to create and manage a simple model of all local and remote devices that are part of the Cisco Service Control solution.

For more information about the Network Navigator, see *Using the Network Navigator* (on page 5-1).

To open the Network Navigator tool:

From the **Tools** menu, choose **Network Navigator**.

The Network Navigator tool opens.



To close the Network Navigator tool:

Right-click on the **Network Navigator** button and, from the short-cut menu, choose **Close**.

The Network Navigator tool closes.

The Service Configuration Editor Tool

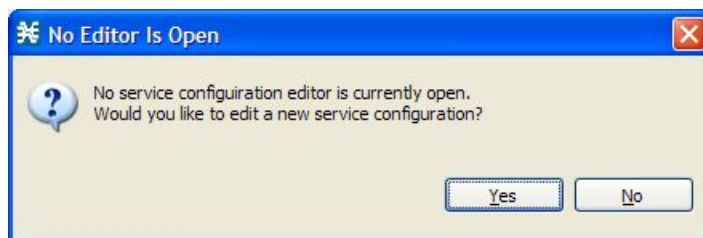
A *service configuration* is a data structure that defines how the SCE platform analyzes network traffic, what rules apply to the traffic, and what actions the SCE platform should take to enforce these rules. The Service Configuration Editor is tool for creating service configurations.

Most of this document discusses using the Service Configuration Editor. Start at *Using the Service Configuration Editor* (on page 6-1).

To open the Service Configuration Editor tool:

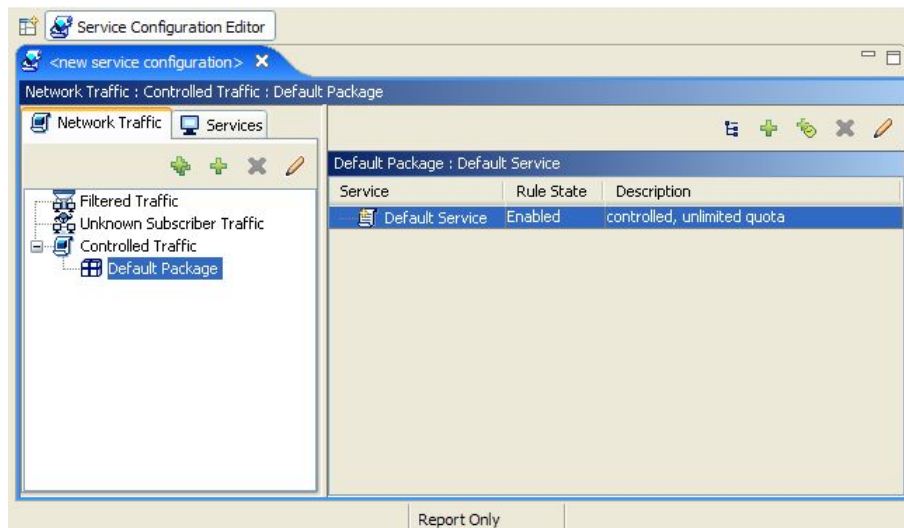
Step 1 From the **Tools** menu, choose **Service Configuration Editor**.

A No Editor Is Open dialog box appears.



Step 2 Click **Yes**.

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



To close the Service Configuration Editor tool:

Right-click on the **Service Configuration Editor** button and, from the short-cut menu, choose **Close**.

The Service Configuration Editor tool closes.

The Signature Editor Tool

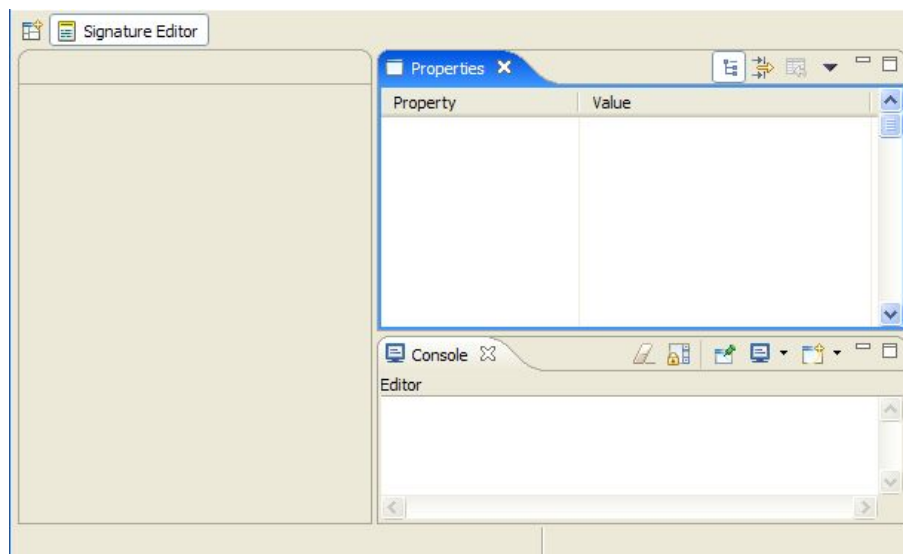
The Signature Editor is a tool that allows you to create and modify files that can add and modify protocols and protocol signatures in *SCA BB*.

For more information about the Signature Editor, see *Using the Signature Editor* (on page 12-1).

To open the Signature Editor tool:

From the **Tools** menu, choose **Signature Editor**.

The Signature Editor tool opens.



To close the Signature Editor tool:

Right-click on the **Signature Editor** button and, from the short-cut menu, choose **Close**.

The Signature Editor tool closes.

The Subscriber Manager GUI Tool

The SM GUI tool allows you to connect to an SCMS-SM, and then manage subscribers, assign packages to subscribers, edit subscriber parameters, and manually add subscribers when dealing with a small number of subscribers.

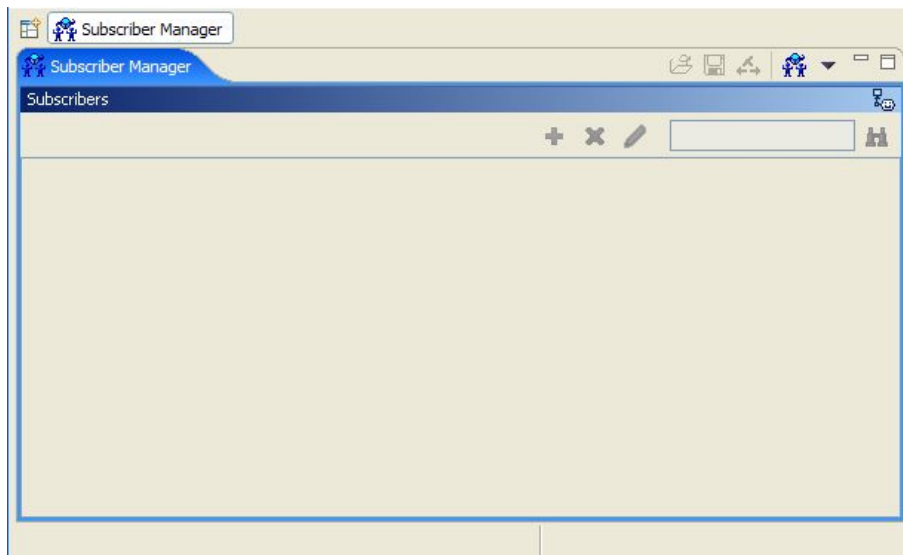
For more information about connecting to an SCMS-SM and using the SM GUI, see *Using the Subscriber Manager GUI Tool* (on page 11-1).

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

To open the SM GUI tool:

From the **Tools** menu, choose **Subscriber Manager**.

The SM GUI tool opens.



Note

To connect to the SCMS-SM, the FTP server on the SCMS-SM device must be enabled on port 21. The connection password is that of the scmscm account.

To close the SM tool:

Right-click on the **Subscriber Manager** button and, from the short-cut menu, choose **Close**.

The SM tool closes.

The Reporter Tool

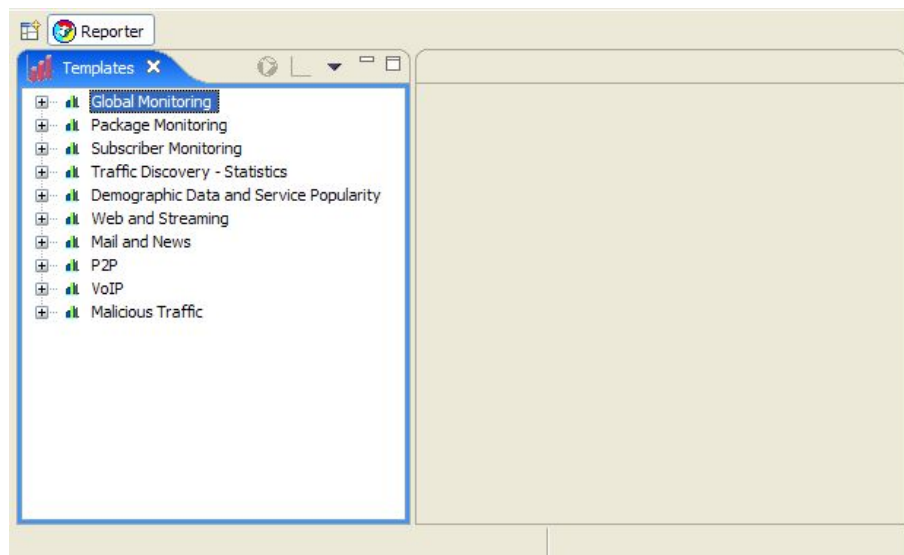
The Cisco Service Control Application Suite (SCAS) Reporter allows you to query the Cisco Service Control Management Suite (SCMS) Collection Manager (CM) RDR database, and present the results in a chart or a table. This is a valuable tool for understanding the habits and resource consumption of the applications and subscribers that use your network. It can also be used for judging 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.

The SCAS Reporter can be run as a standalone or inside the Reporter tool in the SCAS BB Console. For more information about the SCAS Reporter, see the *Cisco Service Control Application Suite Reporter User Guide*.

To open the Reporter tool:

From the **Tools** menu, choose **Reporter**.

The Reporter tool opens.



Note To run the SCAS Reporter, the SCAS BB Console must be connected to the CM.

To close the Reporter tool:

Right-click on the **Reporter** button and, from the short-cut menu, choose **Close**.

The Reporter tool closes.

Accessing On-Line Help

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

To access on-line help:

From the **Help** menu, choose **Help Contents**.

On-line help opens in a separate window.

You can also search on-line help from within the current tool.

To search on-line help:

Step 1 From the **Help** menu, choose **Search**.

A new area containing a Help tab is added 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.

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 on a help topic to view its contents.

You can bookmark topics for later reference.

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

- All topics
 - Related topics
 - Bookmarks
-

Quick Start with the SCAS BB Console

This Quick Start section will help you getting started with the SCAS BB Console. You will add an SCE device to the default site, and apply the default service configuration to the SCE.

Step 1 Launch the SCAS BB Console:

- Choose **start > All Programs > Cisco SCAS > SCAS BB Console 3.0.0 > SCAS BB Console 3.0.0**

Step 2 Open the Network Navigator:

- From the **Tools** menu, choose **Network Navigator**.

This step sets up the SCAS BB Console for network device operations.

Note that the Network Navigator tool is actually opened by default the first time you launch the console.

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

Step 3 Add an SCE device to the default site:

- a) Right-click on the default site, and, from the short-cut menu, select **New > SCE**.

The Create new SCE wizard appears.

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

- c) Click **Finish**.

The new device is added to the site.

Step 4 Check the SCE platform version and operational state:

- a) Right-click on the SCE device and, from the short-cut menu, select **Online Status**.

A Password Management dialog box appears.

- b) Enter the SCE admin password, and click **Extract**.

- c) The SCE online status is retrieved.

- d) Check that the system and application versions are correct, and that the operational state is Active.

Step 5 Open the Service Configuration Editor:

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

A No Editor Is Open dialog box appears.

Step 6 Create a new service configuration:

- Click **Yes**.

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

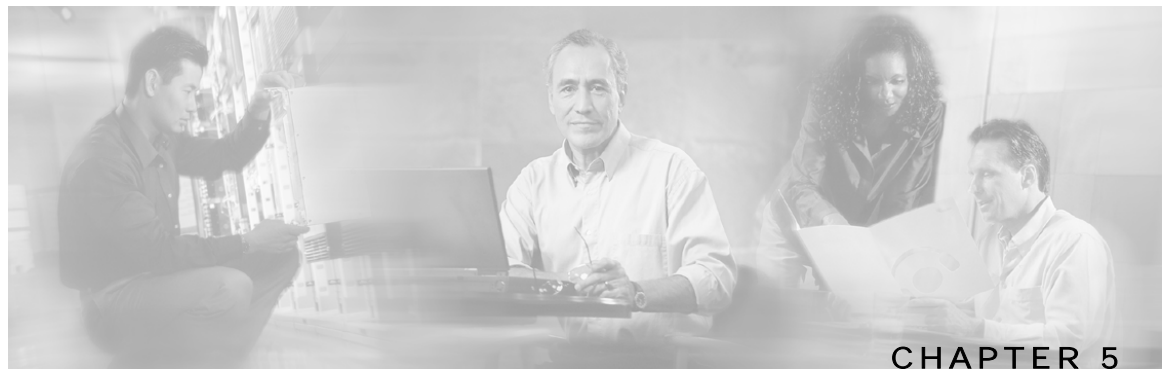
Step 7 Apply the service configuration to the SCE platform:

- a) From the toolbar select  (**Apply Service Configuration to SCE Devices**).

A Password Management dialog box appears.

- b) Enter the SCE admin password, and click **Apply**.

The service configuration is applied to the SCE platform.



Using the Network Navigator

To manage a network entity—Service Control Engine (SCE) platform, Subscriber Manager (SM), or Collection Manager (CM)—from the SCAS BB Console, you must first define it as a device in the Network Navigator. The Network Navigator tool allows you to create a simple model of all local and remote devices that are part of the Cisco Service Control solution, and manage the devices remotely.

This chapter contains the following sections:

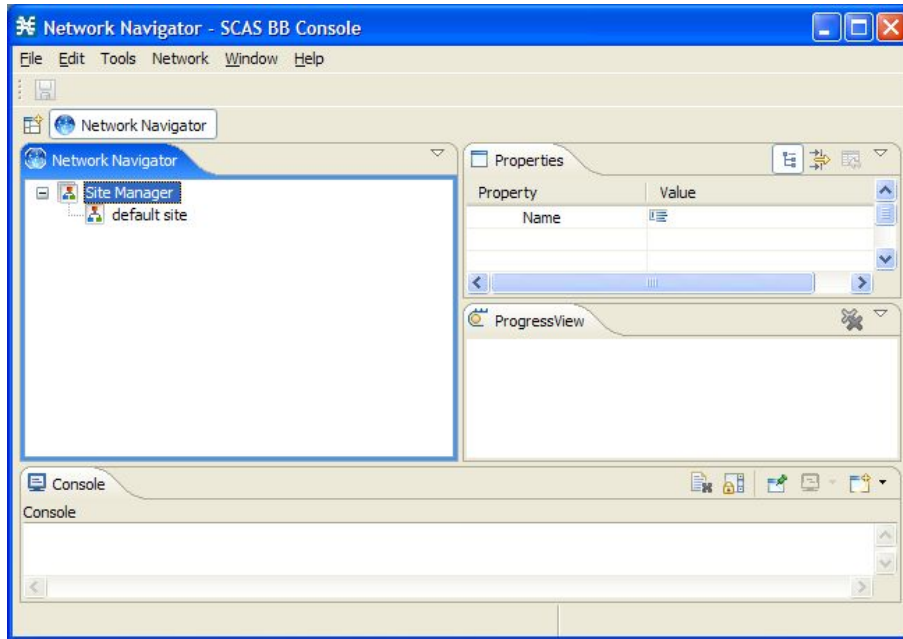
- [The Network Navigator Tool](#) 5-1
- [Managing Sites](#) 5-2
- [Managing Devices](#) 5-6
- [Password Management](#) 5-24
- [Working with Network Navigator Configuration Files](#) 5-24
- [Network Settings Requirements](#) 5-29

The Network Navigator Tool

The Network Navigator tool contains four tabs:

- **Network Navigator**—Displays, in the Site Manager tree, all sites and devices that you have defined as part of your system
- **Properties**—Displays the properties (that can be edited) of the node selected in the Site Manager tree in the Network Navigator tab
- **ProgressView**—When an operation is performed on a site or device in the Site Manager tree, displays a progress bar

- Console—Displays log messages concerning actions performed in the Network Navigator tool



Managing Sites

To be able to manage an SCE, SM, or CM from the SCAS BB Console, each network entity must be defined as a device in the Network Navigator. Once 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.

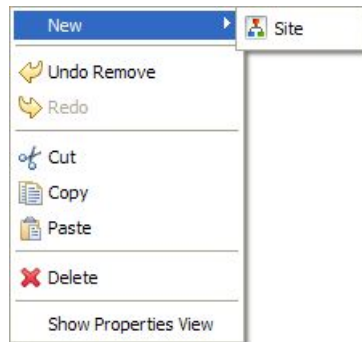
Grouping devices in sites can also help to manage the passwords for these devices (see *Password Management* (on page 5-24)).

Adding a Site to the Site Manager

To add a site to the Site Manager

-
- Step 1** In the Network Navigator tab, right-click on the Site Manager node.

A short-cut 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 tab, enter a name for the site in the Name cell

Step 4 (Optional) In the Version cell, enter a version number.

Adding Devices to a Site

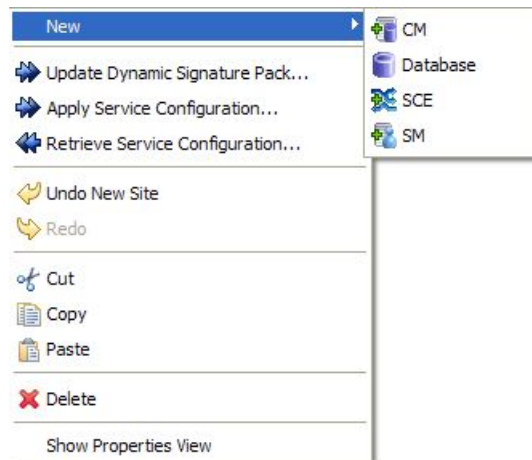
Adding SCE Devices to a Site

To be able to use the Network Navigator to configure, monitor, and update the software of an SCE platform, first add the SCE platform to a site.

To add a SCE device to a site:

Step 1 In the Site Manager tree, right-click on a site.

A short-cut 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** (Optional) In the Name field, enter a meaningful name for the SCE.
- Step 5** Click **Finish**.
The Create new SCE wizard closes
The new device is added to the site
-

Adding SM Devices to a Site

To be able to use the Network Navigator to configure, monitor, and update the software of an SM, first add the SM to a site.

To add a SM device to a site:

-
- Step 1** In the Site Manager tree, right-click on a site.
A short-cut 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** (Optional) 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
-

Adding CM Devices to a Site

To be able to use the Network Navigator to monitor an CM, first add the CM to a site.

To add a CM device to a site:

-
- Step 1** In the Site Manager tree, right-click on a site.
A short-cut 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 Cisco Service Control Management Suite (SCMS) Collection Manager (CM).
- Step 4** (Optional) 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.
-

Adding Database Devices to a Site

To add a database device to a site:

-
- Step 1** In the Site Manager tree, right-click on a site.
A short-cut menu appears.
From the menu select **New > Database**.
The Create new Database wizard appears.
- Step 2** In the Address field, enter the IP address of the Database.
- Step 3** (Optional) In the Name field, enter a meaningful name for the Database.
- Step 4** From the Database type drop-down list, select a database type.
- Step 5** (Optional) Check the Enable Advanced Settings check box and enter new values in the Url, Driver, User, and Password fields.
- Step 6** Click **Finish**.
The Create new Database wizard closes.
The new device is added to the site.
-

Deleting Devices

To delete a device:

-
- Step 1** In the Site Manager tree, right-click on a device.
A short-cut menu appears.

Step 2 From the menu select **Delete**.

The device is deleted; it is removed from the Site Manager tree.

Deleting Sites

To delete a site:

Step 1 In the Site Manager tree, right-click on a site in the Site Manager tree.

A short-cut menu appears.

Step 2 From the menu select **Delete**.

The site and all its devices are deleted; the site is removed from the Site Manager tree.

Managing Devices

Managing SCE Devices

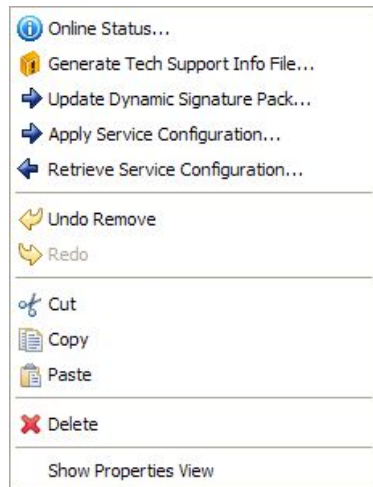
Retrieving the Online Status of SCE Devices

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

To retrieve the online status of an SCE device:

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

A short-cut menu appears.



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

A Password Management dialog box appears.

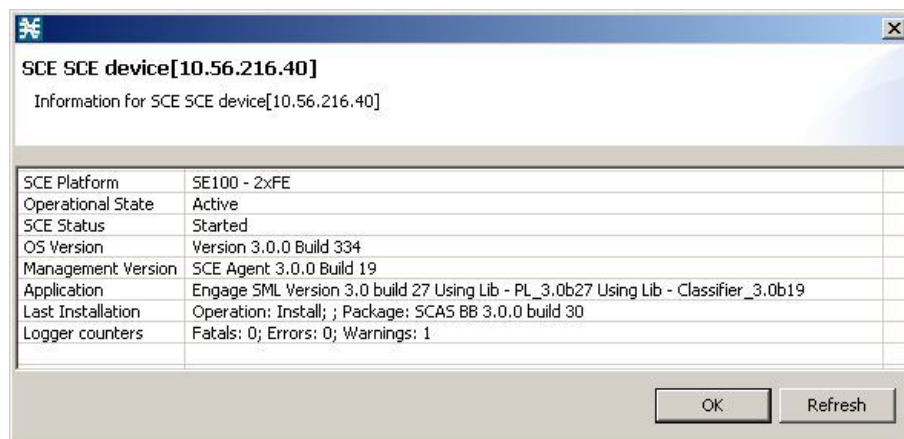
Step 3 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

Step 4 Click **Extract**.

The Password Management dialog box closes.

An Extracting info progress bar appears.

The SCE online status is retrieved.

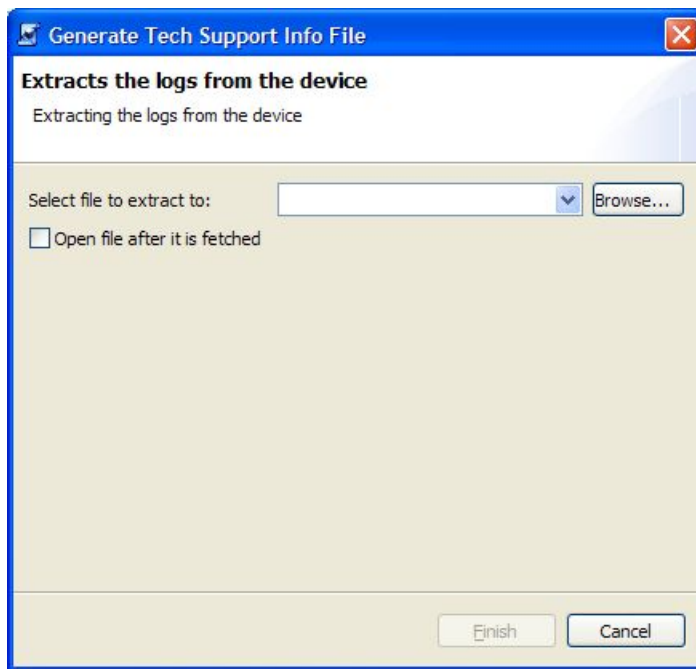


Generating Tech Support Info Files for SCE Devices

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

To generate a tech support info file for an SCE:

-
- Step 1** In the Site Manager tree, right-click on a SCE device.
A short-cut 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 click on an existing ZIP file.
- Step 6** Click **Open** to select the file. If it is an existing file, the contents of the file will be overwritten.
The Select File dialog box closes.
- Step 7** (Optional) Check the Open file after it is fetched check box.
- Step 8** Click **Finish**.
The Generate Tech Support Info File dialog box closes.

A Password Management dialog box appears.

Step 9 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

Step 10 Click **Generate**.

The Password Management dialog box closes.

A Generate tech support info file progress bar appears.

The file is generated.

Installing Protocol Packs on SCE Devices

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 (see *Installing a Protocol Pack* (on page 4-10)).

Applying 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.

To apply a service configuration to a single SCE platform:



Note The service configuration that is to be applied must be open in the Service Configuration Editor.

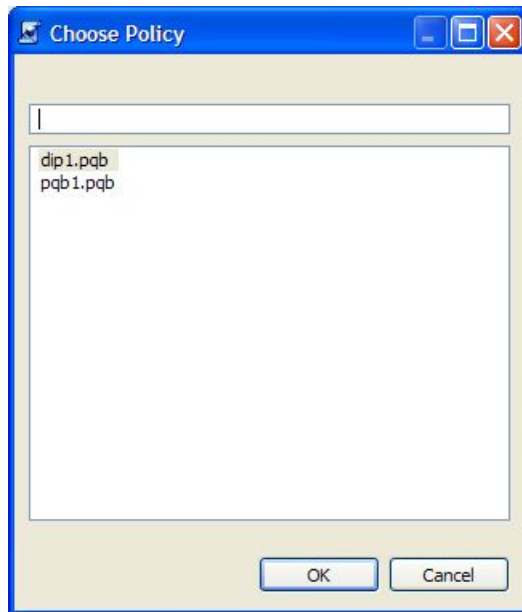
Step 1 In the Site Manager tree, right-click on an SCE device.

A short-cut menu appears.

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

The Choose Policy dialog box appears.

If only one service configuration is open in the Service Configuration Editor, this step is skipped. (If no service configurations are open in the Service Configuration Editor, an error message is displayed.)



All service configurations open in the Service Configuration Editor are listed in the dialog box.

Step 3 Select a service configuration from the list.

Step 4 Click **OK**.

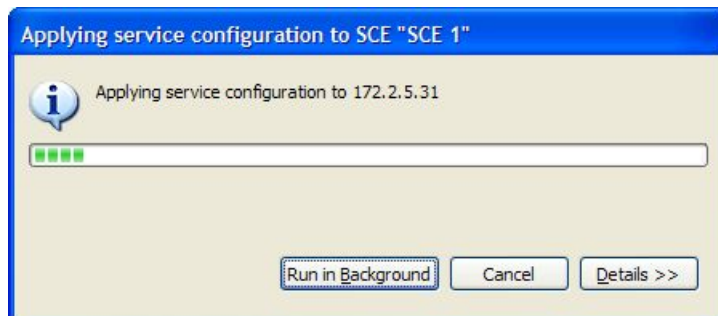
A Password Management dialog box appears.

Step 5 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

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.

To apply a service configuration to multiple SCE platforms:

Step 1 In the Site Manager tree, select sites or SCE devices to which the service configuration is to be applied, right-click on one of them, and, from the short-cut menu that appears, select **Apply Service Configuration**.

The Choose Policy dialog box appears.

Step 2 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 3 For each SCE device, enter the password and click **Apply**.

The service configuration is applied to each selected SCE platform in turn.

Retrieving 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.

To retrieve a service configuration from a single SCE platform:

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

A short-cut menu appears.

Step 2 From the menu select **Retrieve Service Configuration**.

A Password Management dialog box appears.

Step 3 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

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.

To retrieve service configurations from multiple SCE platforms:

- Step 1** In the Site Manager tree, select sites or SCE devices whose service configurations are to be retrieved, right-click on one of them, and, from the short-cut menu that appears, select **Retrieve Service Configuration**.

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

- Step 2** For each SCE device, enter the password and click **Retrieve**.

The service configuration is retrieved from each SCE platform in turn, and opened in the Service Configuration Editor.

Installing PQI Files on SCE Devices

This operation installs the *Cisco Service Control Application for Broadband* on the SCE platform. For more information, see *Installing SCA BB* (on page 4-1).



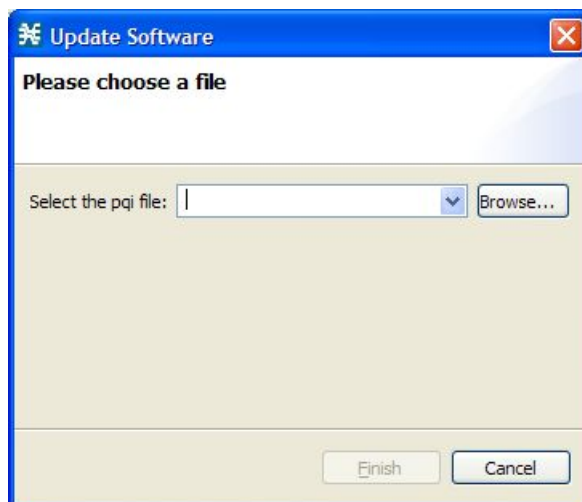
- Note** Installing a PQI file usually takes a few minutes.

To install a PQI file on an SCE device:

- Step 1** In the Site Manager tree, select an SCE device.

- Step 2** From the **Network** menu, choose **Install 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 is to be installed.**Step 5** Click **Open**.

The Select file dialog box closes.

Step 6 Click **Finish**.

A Password Management dialog box appears.

Step 7 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.**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.

Installing the SCE OS Software Package on SCE Devices

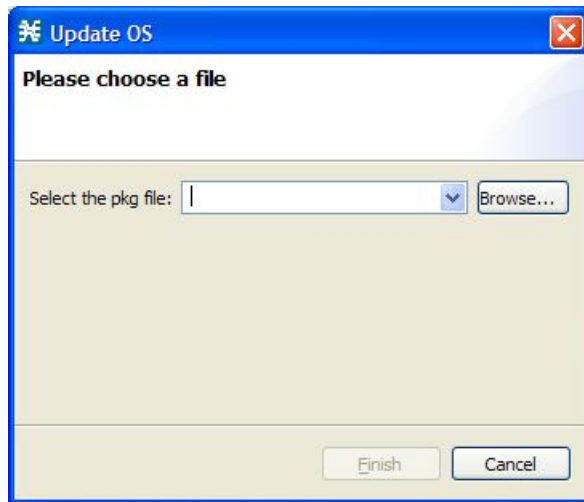
This operation installs the SCE OS software package (the operating system software and firmware of the SCE platform).

For more information, see the section *Upgrading SCE Platform Firmware* in the *Cisco Service Control Engine Software Configuration Guide*.

To install an operating system (OS) file on an SCE device:

Step 1 In the Site Manager tree, select an SCE device.**Step 2** From the **Network** menu, choose **Install OS**.

The Update OS dialog box appears.



Step 3 Click **Browse**.

A Select file dialog box appears.

Step 4 Browse to the PKG file that is to be installed.

Step 5 Click **Open**.

The Select file dialog box closes.

Step 6 Click **Finish**.

A Password Management dialog box appears.

Step 7 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

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

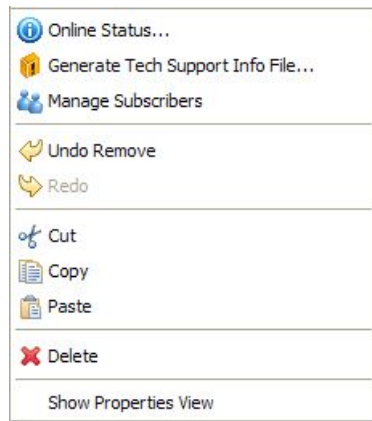
Retrieving the Online Status of SM Devices

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

To retrieve the online status of an SM device:

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

A short-cut menu appears.



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

A Password Management dialog box appears.

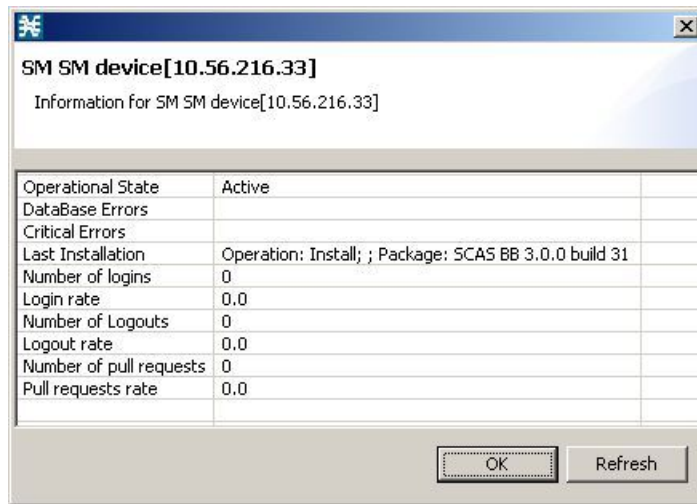
Step 3 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

Step 4 Click **Extract**.

The Password Management dialog box closes.

An Extracting info progress bar appears.

The SCMS-SM online status is retrieved.



Generating Tech Support Info Files for SM Devices

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

To generate a tech support info file for an SM:

- Step 1** In the Site Manager tree, right-click on a SM device.
A short-cut 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 click on an existing ZIP file.
- Step 6** Click **Open** to select the file. If it is an existing file, the contents of the file will be overwritten.
The Select File dialog box closes.
- Step 7** (Optional) Check the Open file after it is fetched check box.
- Step 8** Click **Finish**.
The Generate Tech Support Info File dialog box closes.
A Password Management dialog box appears.

Step 9 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

Step 10 Click **Generate**.

The Password Management dialog box closes.

A Generate tech support info file progress bar appears.

The file is generated.

Managing Subscribers on SM Devices

To manage subscribers:

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

A short-cut menu appears.

Step 2 From the menu select **Manage Subscribers**.

A Password Management dialog box appears.

Step 3 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

Step 4 Click **Connecting**.

The Password Management dialog box closes.

A Connecting to progress bar appears.

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

See *Using the Subscriber Manager GUI Tool* (on page 11-1) for an explanation of how to proceed.

Installing PQI Files on SM Devices



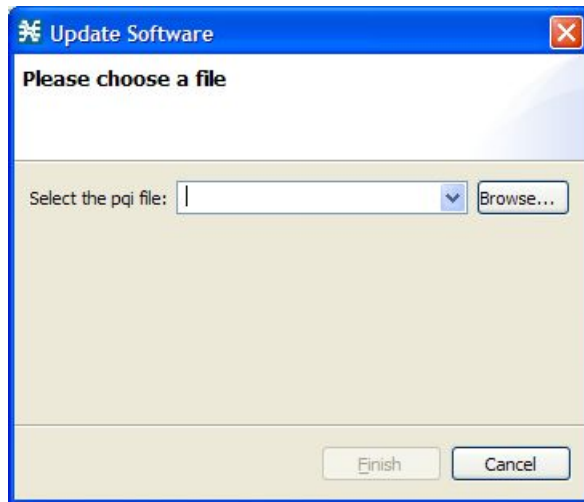
Note Installing a PQI file usually takes a few minutes.

To install a PQI file on an SM device:

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

Step 2 From the **Network** menu, choose **Install 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 is to be installed.

Step 5 Click **Open**.

The Select file dialog box closes.

Step 6 Click **Finish**.

A Password Management dialog box appears.

Step 7 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

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

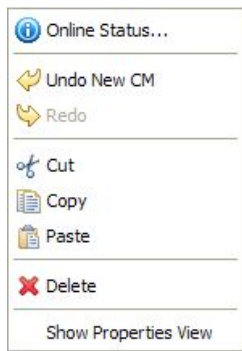
Retrieving the Online Status of CM Devices

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

To retrieve the online status of a CM device:

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

A short-cut menu appears.



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

A Password Management dialog box appears.

Step 3 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

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 screen (for an SCE platform), see *Retrieving the Online Status of SCE Devices* (on page 5-6).

Managing Database Devices

Making Databases Accessible to the SCAS Reporter

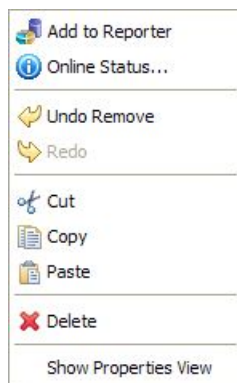
**Note**

An alternative procedure is described in the *Cisco Service Control Application Suite Reporter User Guide*.

To make other databases accessible to the SCAS Reporter:

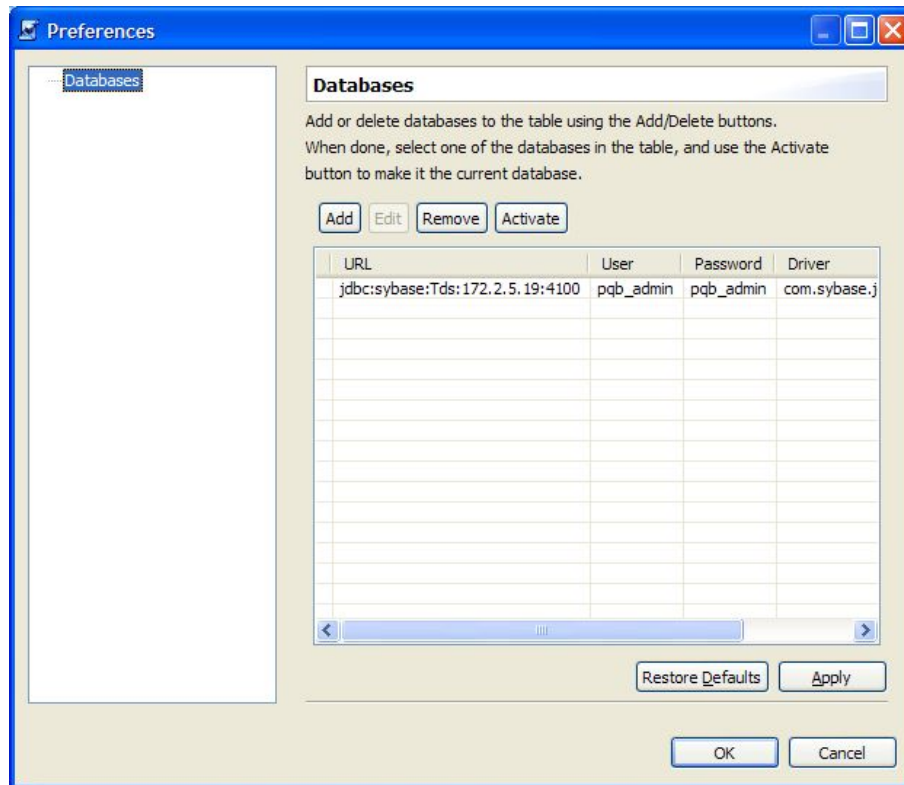
Step 1 In the Site Manager tree, right-click on a database device.

A short-cut menu appears.



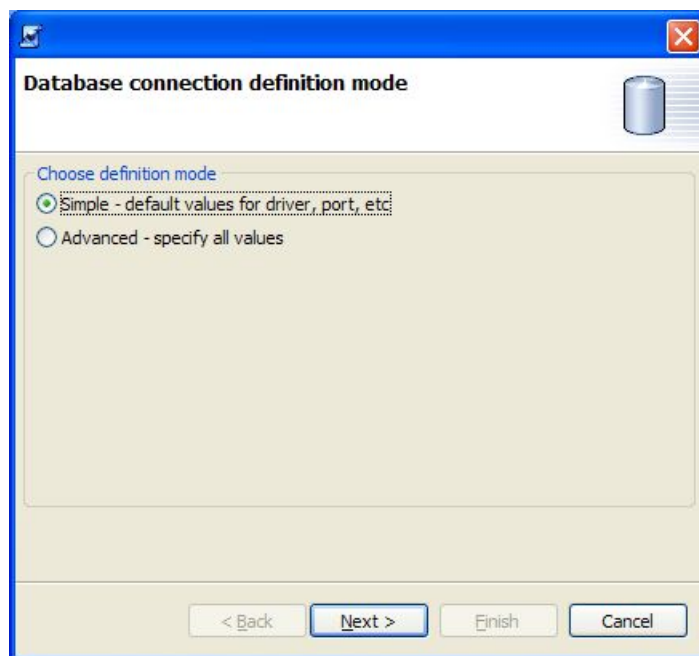
Step 2 From the menu select **Add to Reporter**.

The Preferences dialog box appears.



Step 3 Click **Add**.

A wizard appears.



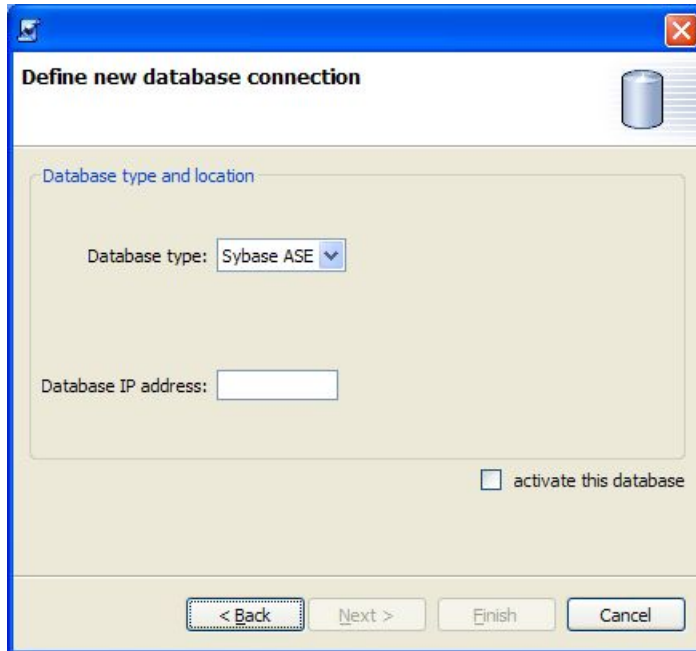
Step 4 Select a definition mode radio button:

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

Step 5 Click **Next**.

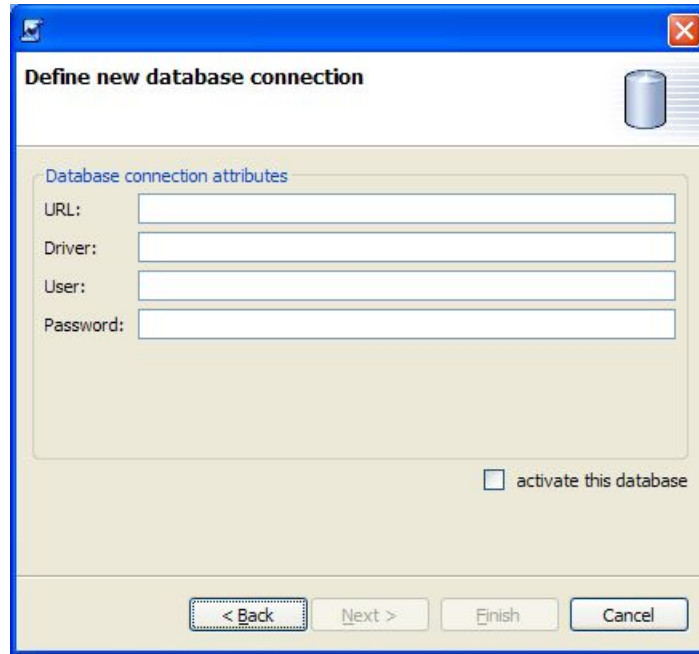
The final screen of the wizard appears. The actual screen depends on the definition mode you selected in step 4:

- The simple screen:



The screenshot shows a dialog box titled "Define new database connection". The dialog has a blue title bar with standard window controls. Below the title bar, there is a section titled "Database type and location" with a database cylinder icon. Inside this section, there is a "Database type:" label followed by a dropdown menu currently set to "Sybase ASE". Below that is a "Database IP address:" label followed by an empty text input field. At the bottom right of the section, there is a checkbox labeled "activate this database" which is currently unchecked. At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- The advanced screen:



Step 6 Fill in all the fields.

Step 7 Click **Finish**.

The wizard closes.

The definition of the database is added to the list in the Preferences dialog box.

Step 8 Repeat steps 3 to 7, as required.

Step 9 Remove database connection information, if necessary.

Step 10 Make sure that the correct database is activated.

Step 11 Click **OK**.

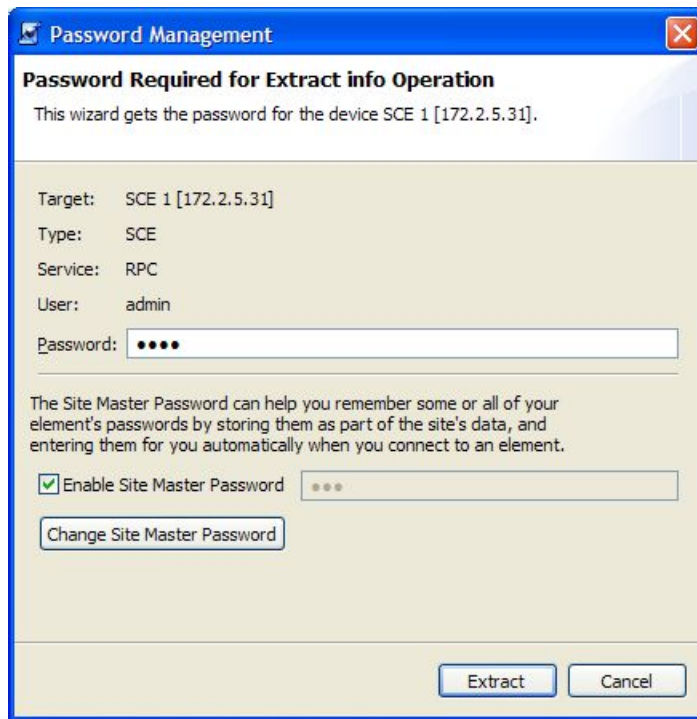
The Preferences dialog box closes.

Password Management

Normally, you must enter the password for a device before the device can be accessed. When you try to perform any operation with a site device, the Network Navigator first asks for the device 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 a tedious task. The Site Master Password can help you remember some or all of your element's passwords by storing them as part of the site's data, and entering them for you automatically when you connect to an element.

The Site Master Password protects saved passwords in the password manager. The SCAS BB Console 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.



For each site, when the Password Management dialog box appears, check the Enable Site Master Password check box.

Working with Network Navigator Configuration Files

Once sites and devices have been added 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 SCAS BB Console.

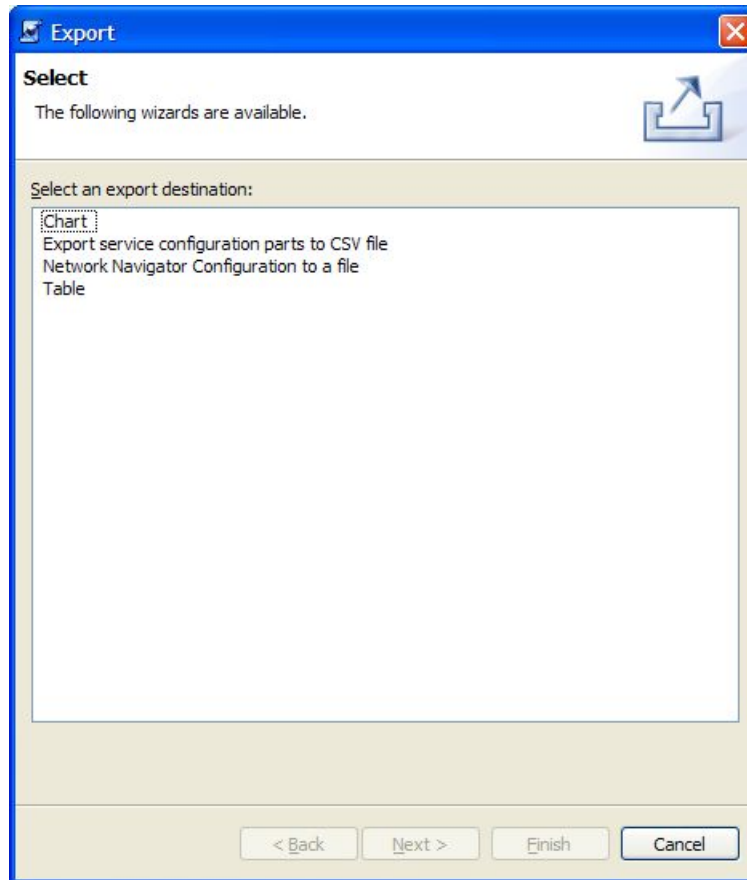
If you use the Site Master Password to store the passwords of the network devices, the passwords are also exported, in encrypted form. This means that other users who import this data need only provide the Site Master Password to access the devices.

Exporting a Network Navigator Configuration

To export a Network Navigator configuration to a file:

Step 1 From the **File** menu, choose **Export**.

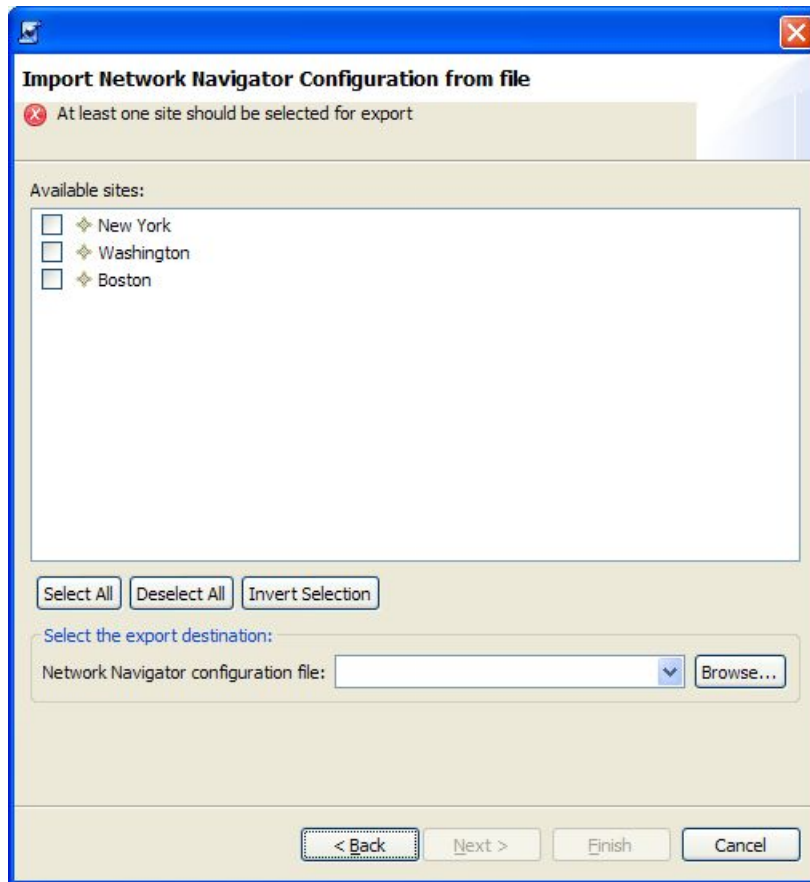
The Export dialog box appears.



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 click on an existing `site.xml` file.

Step 8 Click **Open** to select the file.

If it is an existing file, the contents of the file will be overwritten.

The Open dialog box closes.

Step 9 Click **Finish**.

The Export Network Navigator Configuration dialog box closes.

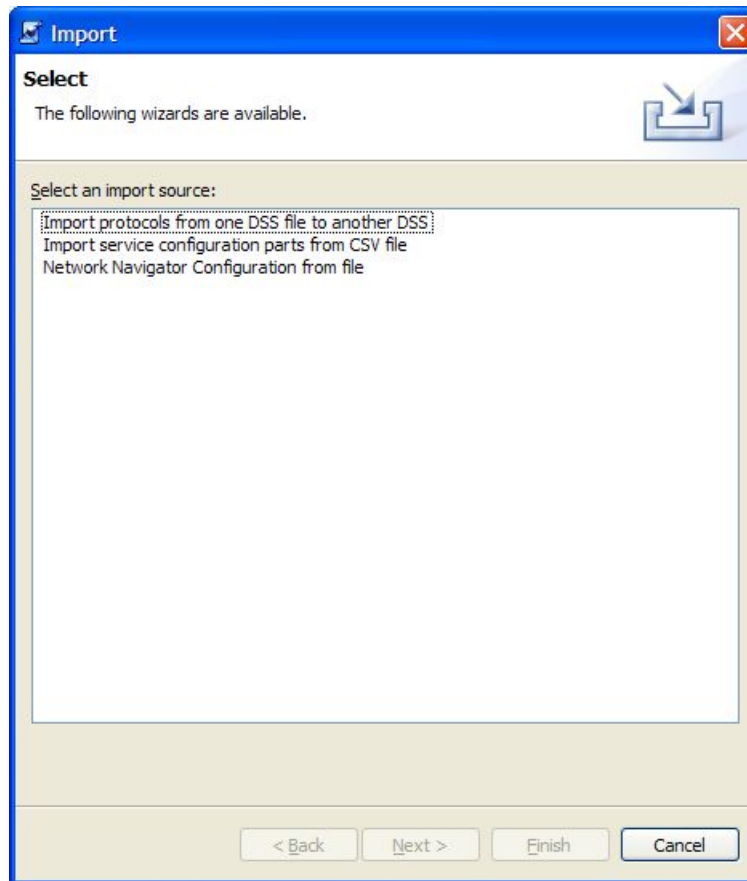
The configuration is saved to the file.

Importing a Network Navigator Configuration

To import a Network Navigator configuration to a file:

Step 1 From the **File** menu, choose **Import**.

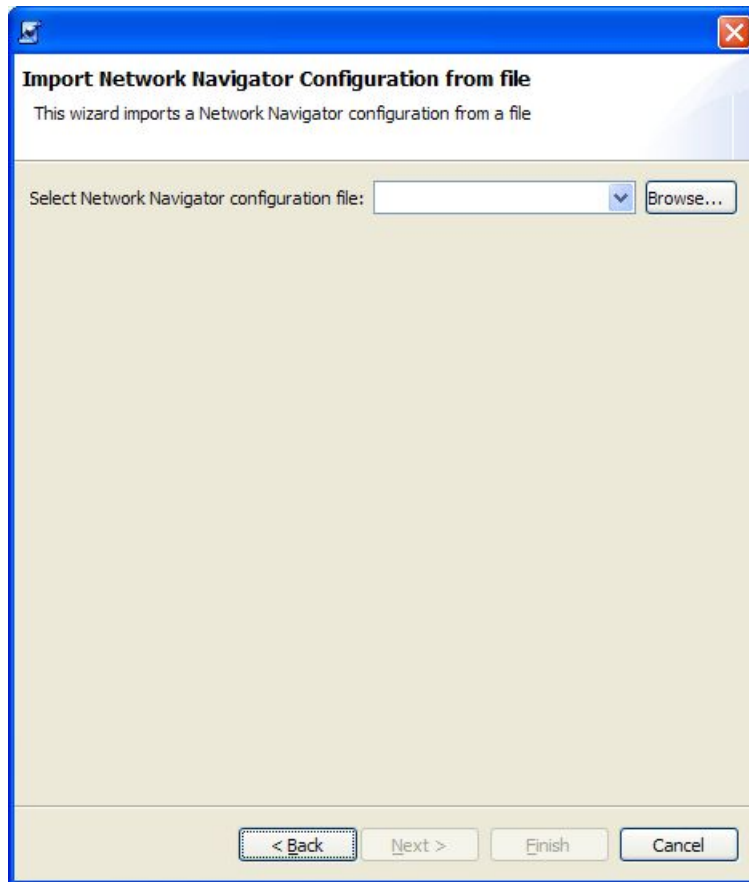
The Import dialog box appears.



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 click on 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

The following are the firewall/NAT open port settings required for the Network Navigator to operate properly:

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: <ul style="list-style-type: none"> • Install OS • Generate Tech Support Info File
SCE	Workstation ports 21000 - 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	SM port 21/TCP	FTP—Required for SM authentication
Workstation	CM port 14375/TCP	PRPC—Required for the CM Online Status operation
Workstation	CM port 21/TCP	FTP—Required for CM authentication

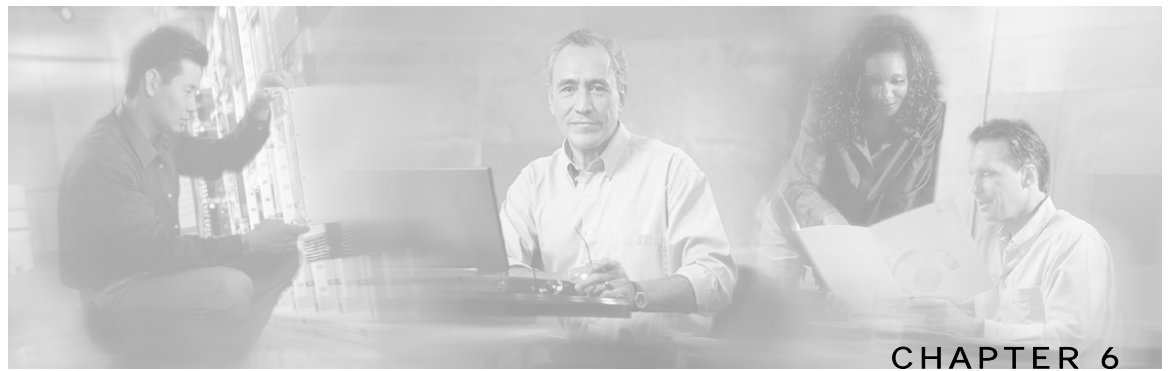
The SCAS Reporter may have additional requirements for connecting to the database. See the *Cisco Service Control Application Suite Reporter User Guide* for more information.

User Authentication

The following are the user authentication methods used by the Network Navigator:

Destination	Username	Password	Comments
SCE	admin (fixed)	The SCE admin (enable 10) password	Authentication is performed over PRPC
SM	pcube (fixed)	The password of the pcube FTP user on the SM machine	Authentication is performed over FTP
CM	scmscm (fixed)	The password of the scmscm FTP user on the CM machine	Authentication is performed over FTP

You must activate an FTP server on the SM and CM machines and define the appropriate users for authentication to succeed.



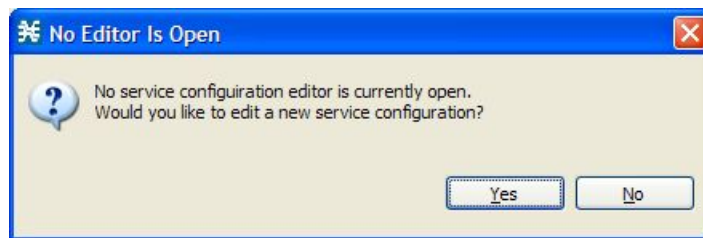
Using the Service Configuration Editor

This chapter contains the following sections:

- [The Service Configuration Editor Tool](#) 6-1
- [Managing Service Configurations](#) 6-2

The Service Configuration Editor Tool

When you first open the Service Configuration Editor tool, a No Editor Is Open dialog box appears.



- To create a new service configuration (see *Adding New Service Configurations* (on page 6-2)) click **Yes**.
- To open an existing service configuration (see *Opening Existing Service Configurations* (on page 6-3)) click **No**.

When you first add or open a service configuration, the Configuration option is added to the main menu.

You can have many service configurations open at one time; each is displayed in its own tab, and you click on a tab to select the active service configuration.

When a service configuration has unsaved changes, its name on the tab is preceded by an asterisk.

Managing Service Configurations

A *service configuration* is a data structure that defines how the Service Control Engine (SCE) platform analyzes network traffic, what rules apply to the traffic, and what actions the SCE platform should take 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 should act upon transactions from different services

Service configurations are stored as PQB files.

Adding New Service Configurations

Remove progress bar

You can add a new service configuration whenever necessary.



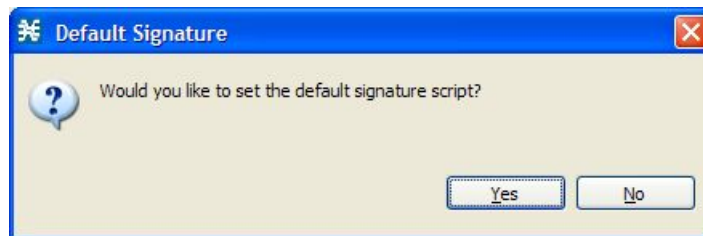
Note

You cannot add a second new service configuration until you have saved the first one.

To add a new service configuration:

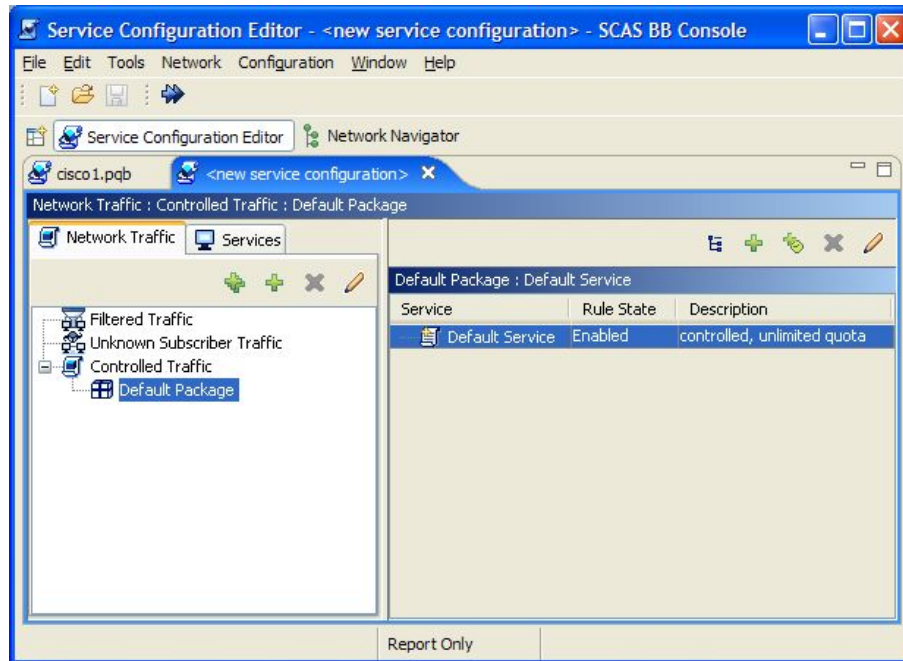
In the toolbar, click  (**New Service Configuration**)

- If a default DSS file is installed (see *The Default DSS File* (on page 7-37)), 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 SCAS BB Console window, open on the Network Traffic tab, and becomes the active service configuration.




When a new service configuration opens, it contains the default service configuration supplied with *SCA BB*. This includes a Default Package; the Default Package contains a Default Service rule.

Opening Existing Service Configurations

Use this operation to open a saved service configuration for viewing or editing, or applying to an SCE platform.

Service configuration files have extension PQB.

To open a service configuration file:

- Step 1** Do one of the following:
- From the **File** menu, choose **Open Service Configuration**
 - In the toolbar, click  (**Open A Service Configuration File**)

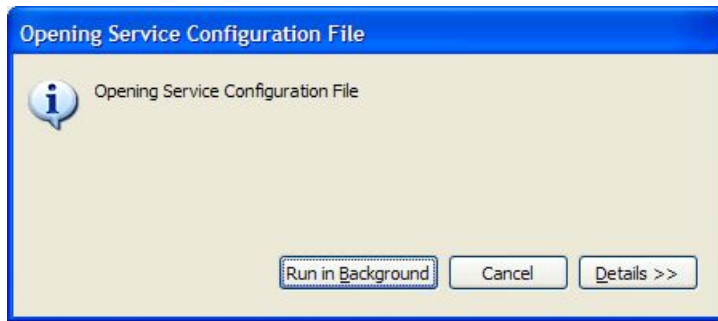
An Open dialog box appears.

Step 2 Browse to a service configuration file.

Step 3 Click **Open**.

The Open dialog box closes.

An Opening Service Configuration File message appears.



The service configuration is loaded into the console:

- This service configuration is active
- The title of the console window changes to display the name of the active service configuration

Saving the Current Service Configuration

Use this procedure to save the active service configuration.

To save the current service configuration to a service configuration file:

Step 1 From the **File** menu, choose **Save As**.

A Save As dialog box appears.


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 click on an existing PQB file.

Step 4 Click **Save** to save the service configuration to the selected file. If it is an existing file, this service configuration overwrites the contents of the file.

During processing a Saving Service Configuration File message appears.


To save the current service configuration to the file from which it was loaded:

In the toolbar, click  (**Save**).

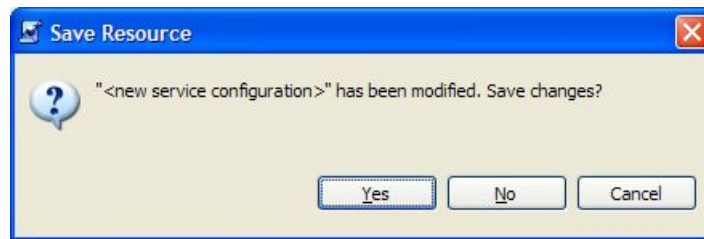
If the current service configuration was not loaded from a PQB file (that is, it is new, or was retrieved from an SCE platform), the Save As dialog box opens as in the previous procedure.

Closing Service Configurations

To close a service configuration:

On a service configuration tab, click  (**Close**).

- If there are no unsaved changes, the service configuration tab closes
- If there are unsaved changes:
 - a) A Save Resource message appears.



b) Click **Yes**.

- If this is an existing edited service configuration, the changes are saved and the service configuration tab 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 tab closes
-

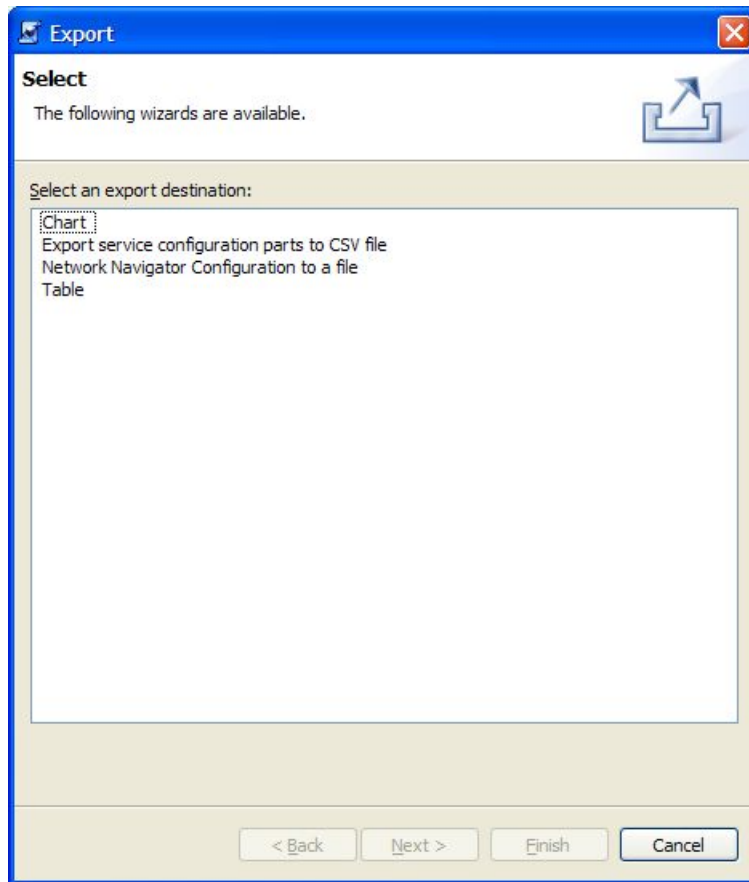
Exporting Service Configuration Data

Use this option to export service configuration data from the current service configuration to CSV files. The CSV file formats are described in the *Cisco Service Control Application Suit for Broadband Reference Guide*.

To export one type of service configuration element to a CSV file:

Step 1 From the **File** menu, choose **Export**.

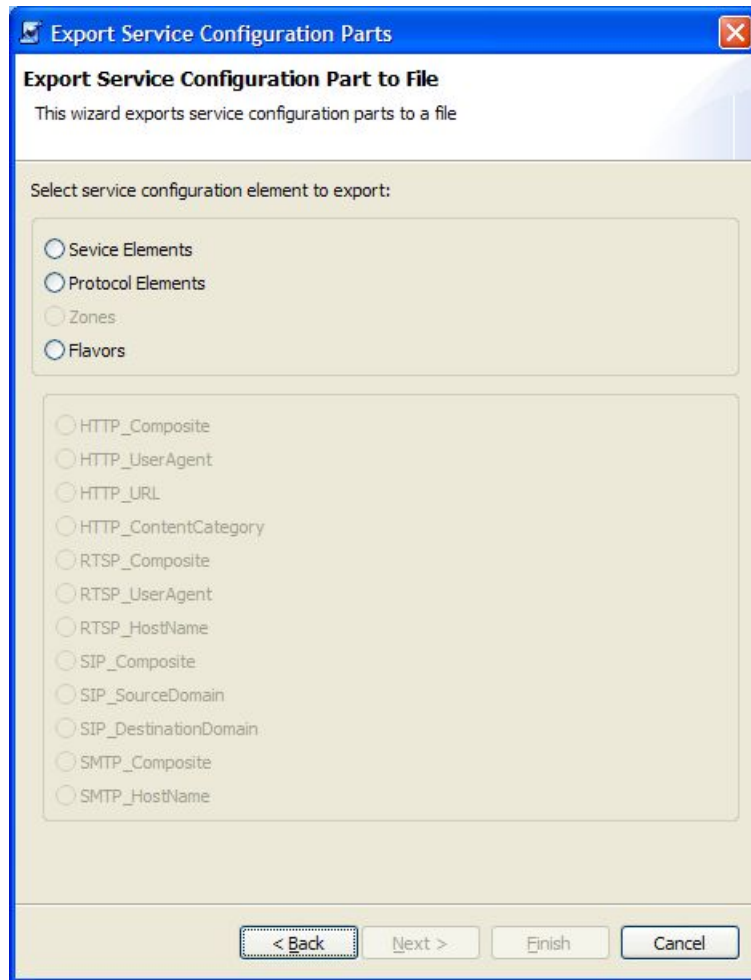
The Export dialog box appears.



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 In the Select service configuration element to export area, click one of the **service configuration element** radio buttons:

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

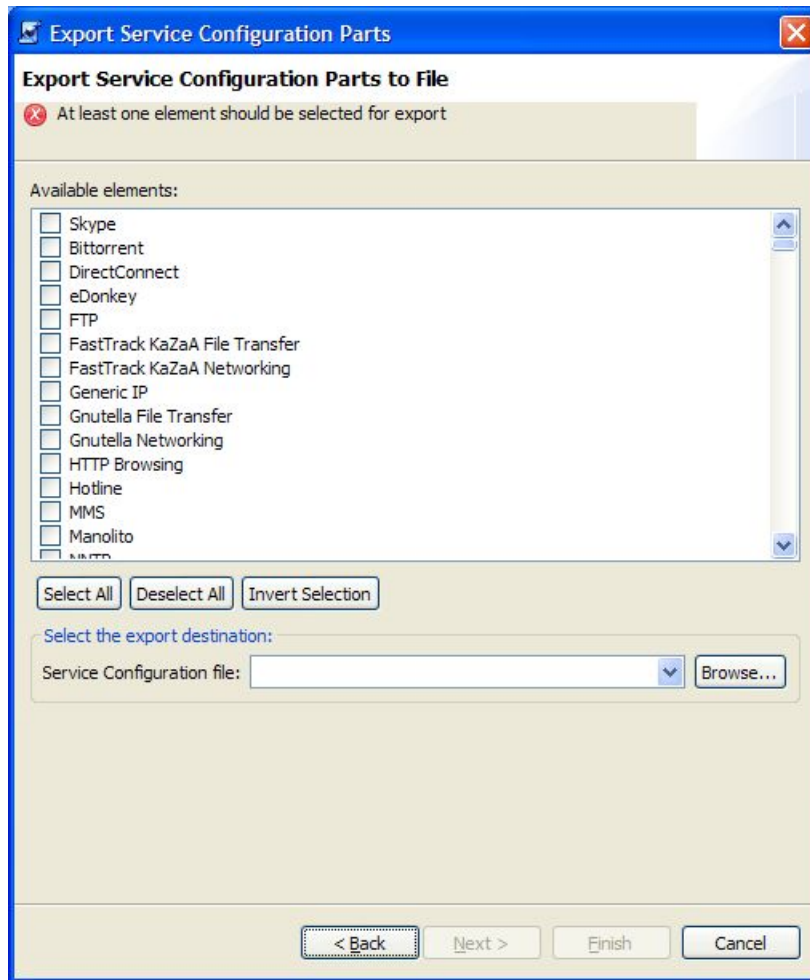
If you selected Flavors, the flavors in the flavor area of the dialog box are enabled.

Only those flavors for which a flavor type is defined in this service configuration are enabled.

Step 5 If you selected Flavors, click one of the **flavor type** radio buttons.

Step 6 Click **Next**.

The second screen of the Export Service Configuration Parts dialog box appears.



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 click on an existing CSV file.

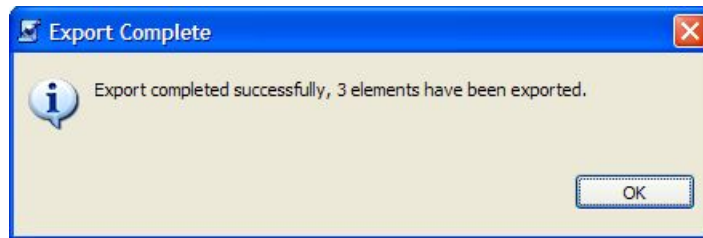
Step 11 Click **Open** to select the file. If it is an existing file, the contents of the file will be overwritten.

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.

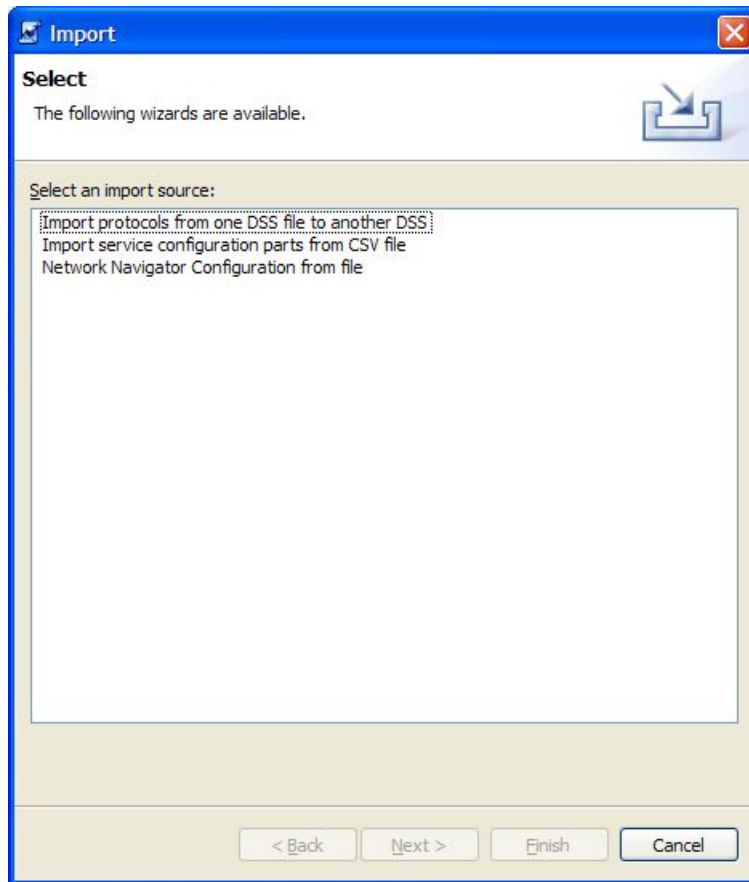
Importing Service Configuration Data

Use this option to import service configuration data to the current service configuration from CSV files. The CSV file formats are described in the *Cisco Service Control Application Suit for Broadband Reference Guide*.

To import one type of service configuration element from a CSV file:

Step 1 From the **File** menu, choose **Import**.

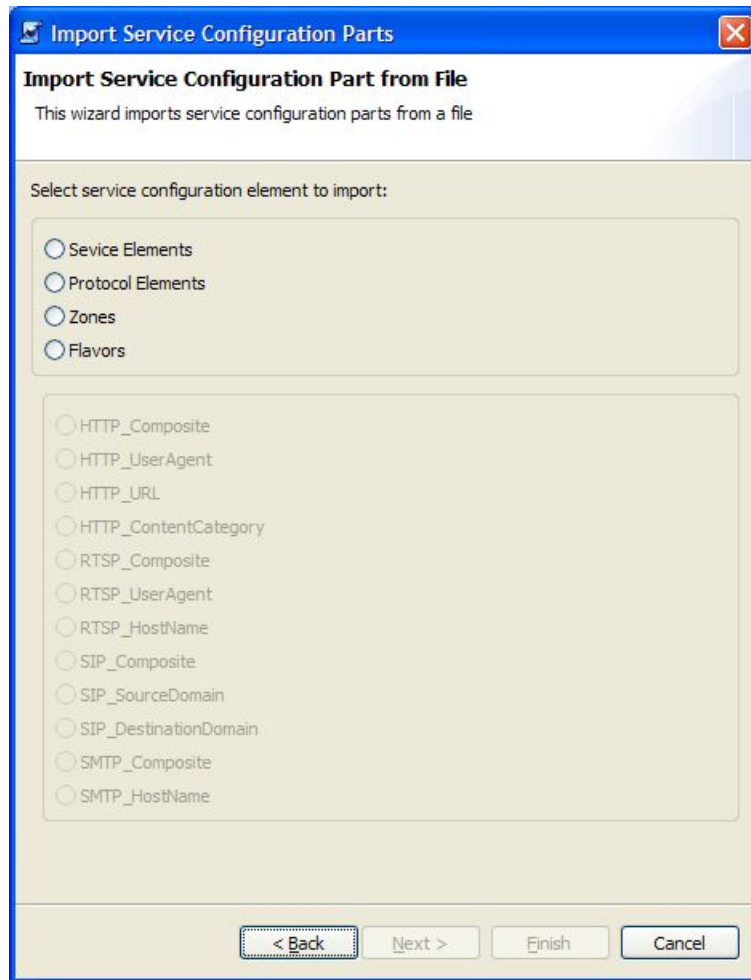
The Import dialog box appears.



Step 2 From the export destination list, select **Import service configuration parts from CSV file**.

Step 3 Click **Next**.

The Import Service Configuration Parts dialog box appears.



Step 4 In the Select service configuration element to import area, click one of the **service configuration element** radio buttons:

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

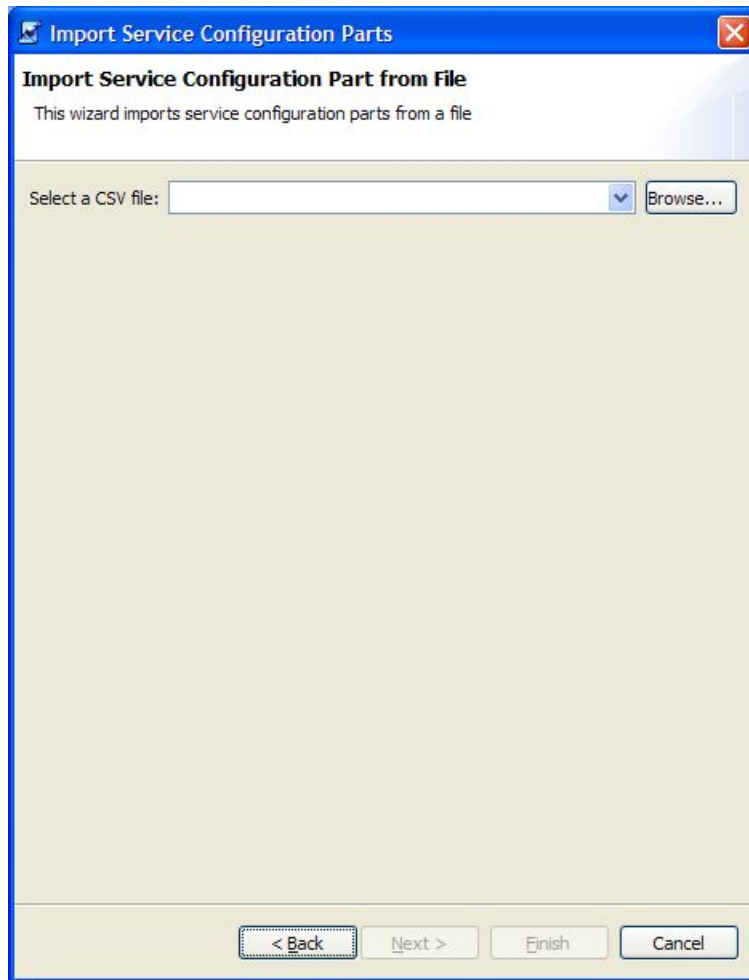
If you selected Flavors, the flavors in the flavor area of the dialog box are enabled.

Only those flavors for which a flavor type is defined in this service configuration are enabled.

Step 5 If you selected Flavors, click one of the **flavor type** radio buttons.

Step 6 Click Next.

The second screen of the Import Service Configuration Parts dialog box appears.



Step 7 Click **Browse**.

An Open dialog box appears.

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

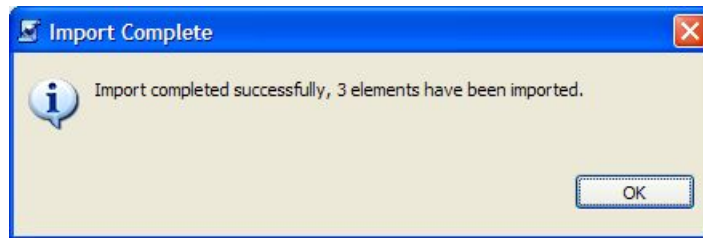
Step 9 Click **Open** to select the file.

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

A service configuration must be applied to the SCE platform. If you do not apply the service configuration, the new or edited service configuration does not take effect, and the previous service configuration continues to be enforced by the SCE platform.

You can apply a service configuration to an SCE platform from the Service Configuration Editor. You *cannot* retrieve a service configuration using the Service Configuration Editor.

You can apply or retrieve a service configuration *using the Network Navigator* (on page 5-1).

You can also apply or retrieve a service configuration using *servconf*, the **SCA BB** Service Configuration Utility. This utility provides an easy method for automating the application and retrieval of service configurations. (See *Using the SCA BB Service Configuration Utility* (on page 13-1).)

Validating the Current Service Configuration

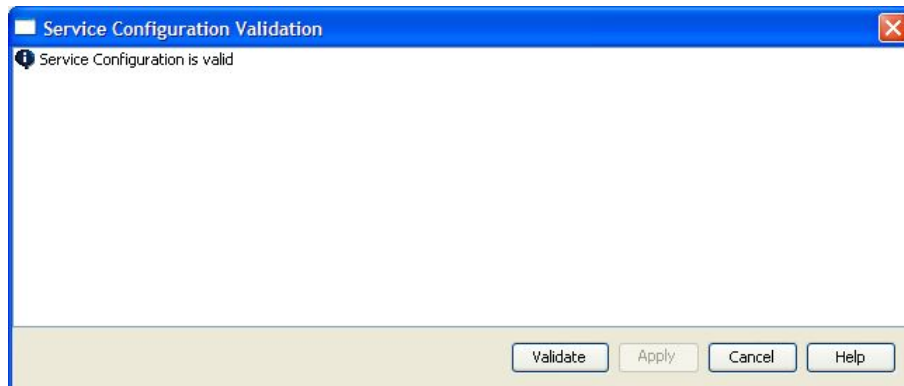
Use the Validate option to validate the new or updated service configuration currently displayed. The validation process checks for overall service configuration coherence, and points out possible pitfalls within the service configuration.

The Validate process is also run automatically when you select Apply Service Configuration to SCE devices. The service configuration is validated and the Service Configuration Validation dialog box appears only if the procedure found errors or issued warnings regarding the current service configuration.

To validate the current service configuration:

Step 1 From the **File** menu, choose  (**Validate**).

The Service Configuration Validation dialog box appears.



Any problems with the service configuration are listed in the dialog box.

Step 2 Click **Cancel**.

The Service Configuration Validation dialog box closes.

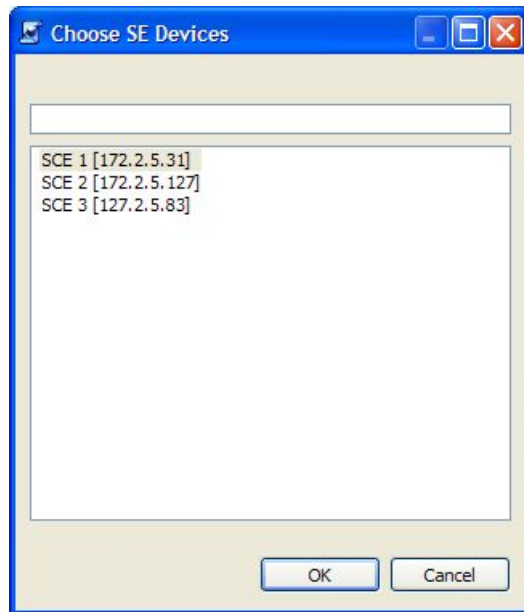
Applying a Service Configuration to SCE Platforms

When you click **Apply Service Configuration to SCE Devices**, the service configuration is validated. If there is a problem and the validation process ends with a warning or error, the Service Configuration Validation screen appears, supplying the validation results. Select **Apply** or correct the problem prior to applying the service configuration. Use the **Validation** menu command to manually validate a service configuration at any time.

To apply the current service configuration to SCE platforms:

Step 1 In the toolbar, click  (**Apply Service Configuration to SCE Devices**).

The Choose SE 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.

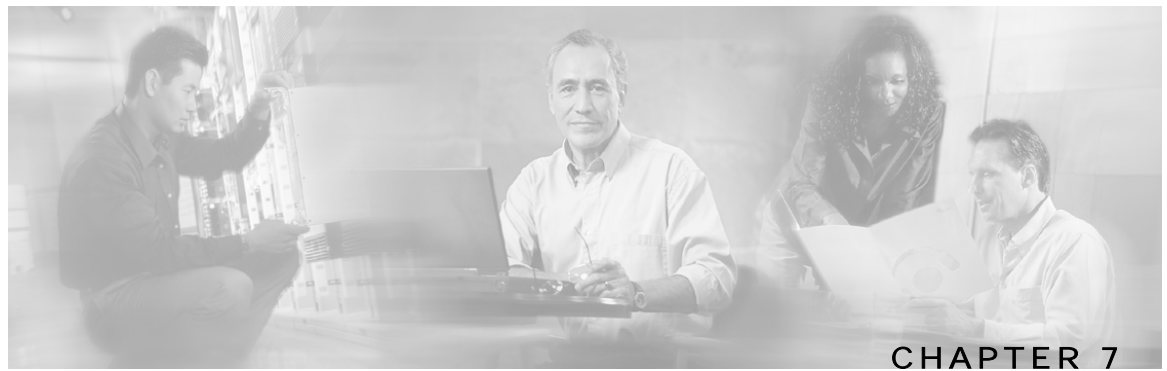
Step 4 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

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 service configuration is applied to the selected SCE platforms.



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. This service is used to classify and identify the traffic, report on its usage, and control it, as required.

It is recommended that you first define a variety of services and only then define your packages. However, the instructions in this chapter are independent of those in the section on adding new packages (see *Managing Packages* (on page 9-1)).

This chapter now explains how to work with services and their elements and sub-elements.

This chapter contains the following sections:

- [Managing Services](#) 7-1
- [Managing Protocols](#) 7-20
- [Managing Zones](#) 7-42
- [Managing Flavors](#) 7-48

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**—Using the Service Control Engine (SCE) platform application-protocol awareness, the system classifies network traffic according to the protocol used
- **Initiating side**—Transactions can be classified to different services according to where they were initiated
- **Zone**—IP addresses of the network-side host of the transaction

- Flavor—Specific Layer 7 properties; for instance, hostnames of the network-side host of the transaction

Services have the following limitations:

- There can be a maximum of 500 services in a service configuration
- There can be a maximum of 10,000 service elements in a service configuration
- Every service element must be unique

Service Parameters

A service is defined by the following parameters:

- General parameters:
 - Name—Each service must have a unique name.
 - Description—An optional description of the service.
- Hierarchy parameters:
 - Parent Service—The parent service is important when services share usage counters. The Default Service is the base of the service hierarchy, and does not have a parent.
 - Service Usage Counters—Usage counters are used by the system when it generates data about the total use of each service. A service can use exclusive global and subscriber usage counters, or use the usage counters of the parent service.

Each usage counter has a name assigned by the system (based on the service name), and a unique counter index. A default value of the counter index is provided by the system; you should not modify this value.
- Advanced parameter:
 - Service Index—Each service has a unique service index. The system recognizes services by their index number; changing the service name does not affect SCE platform activity. A default value of the service index is provided by the system; you should not modify this value.

These parameters are defined when you add a new service (see *Adding Services* (on page 7-4)), and can be changed at any time (see *Editing Services* (on page 7-8)).

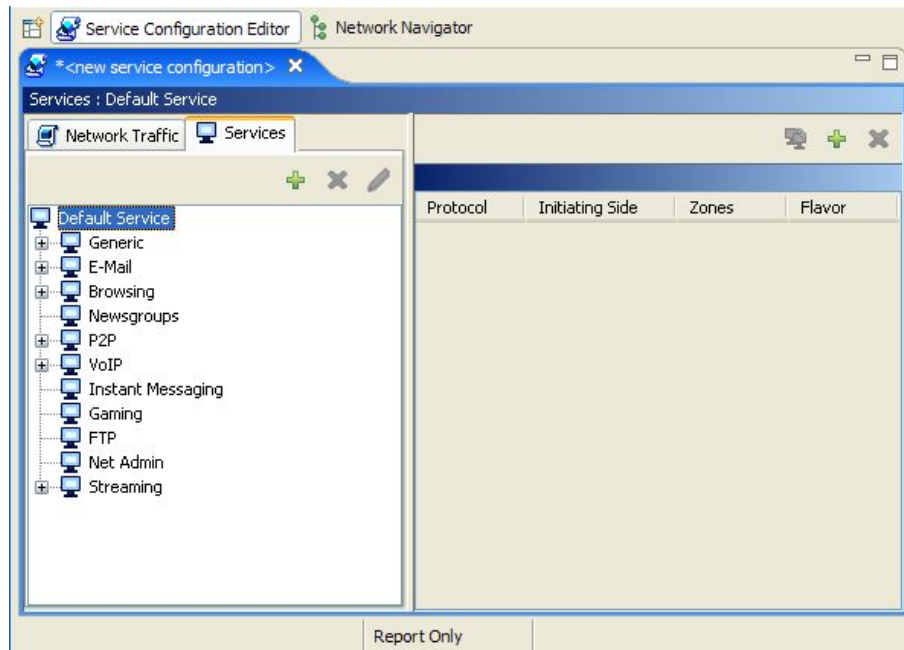
Viewing Services

You can view a hierarchy tree of all existing services, and also see their associated service elements.

To view all services:

Step 1 In the current service configuration, click the **Services** tab.

The Services tab appears.

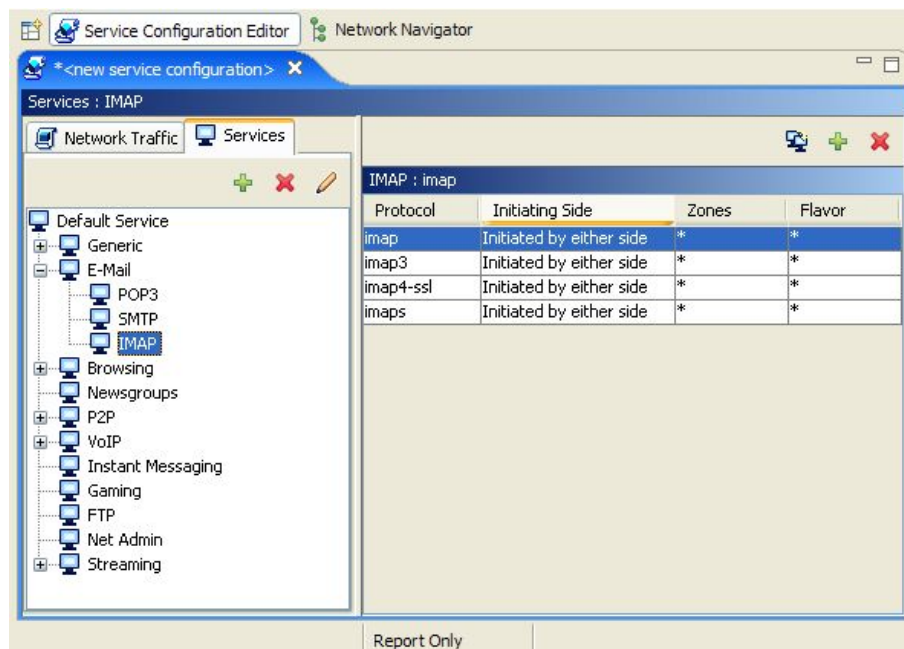


A list of all services is displayed in the services hierarchy.

To view more information about a service, open the Service Settings dialog box (*see Editing Services* (on page 7-8)).

Step 2 Click on a service in the hierarchy to display its service elements.

A list of all service elements defined for this service appears in the Service Element pane.



Adding Services

A number of services are predefined in the SCAS BB Console installation. You can add additional services to the service configuration.

Adding a service to the Services hierarchy is the first step in defining a new service.

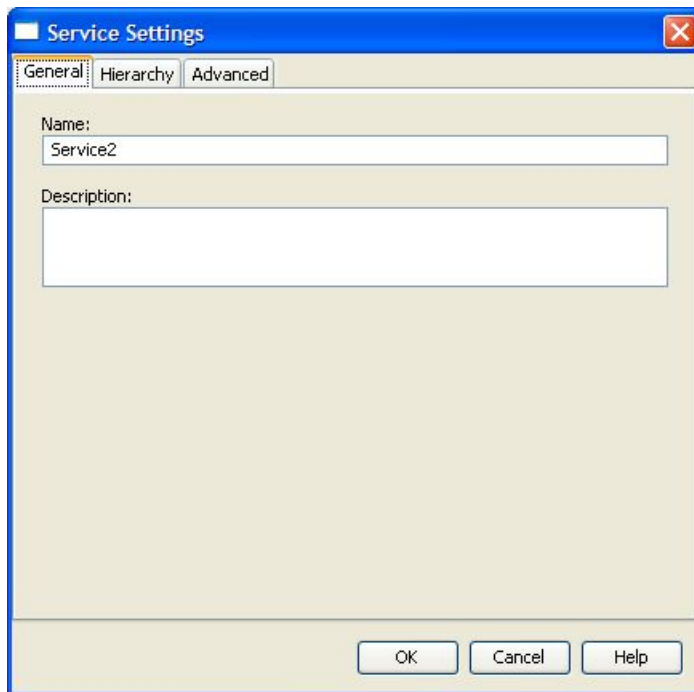
Once you have added and defined a new service, you can add service elements to the service (see *Adding Service Elements* (on page 7-10)).

To add a service to the service configuration:

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

Step 2 In the Services tab, click **+** (**Add Service**).

The Service Settings dialog box appears.



This dialog box has the following tabs: General, Hierarchy, and Advanced.

Step 3 To begin defining the service, continue with the instructions in the section *Defining General Parameters for a Service* (on page 7-5).

Defining General Parameters for a Service

Having added a service to the service hierarchy, you must now set values for its parameters.

To set the name and description of the service:

When you added the service to the service hierarchy, the Service Settings dialog box appeared, open on the General tab.

- Step 1** In the Name field, enter a unique and relevant name for the service.
- Step 2** (Optional) In the Description field, enter a meaningful and useful description of the service.
- Step 3** To set exclusive usage counters for this service, or if you did not select the proper parent service when adding the service, continue with the instructions in the section *Defining Hierarchical Settings for a Service* (on page 7-5).
- Step 4** Click **OK**.
The Service Settings dialog box closes.

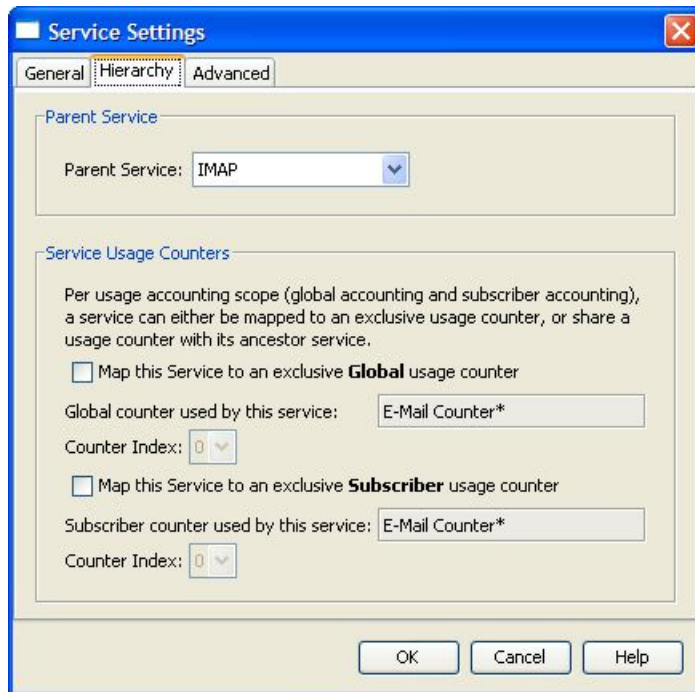
The service is added to the service hierarchy as a child to the service selected in the hierarchy.

Defining Hierarchical Settings for a Service

To select a parent service and set the service usage counters:

-
- Step 1** In the Service Settings dialog box, click the **Hierarchy** tab.

The Hierarchy tab of the Service Settings dialog box appears.



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 usage counters.) To define an exclusive global usage counter:

a) 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.

b) (Optional) Select a value for the counter index from the Counter Index drop-down list.

A default value of the counter index is provided by the system; you should not modify this value.

Step 4 To define an exclusive subscriber usage counter:

- Repeat step 3 for the subscriber usage counter section of the dialog box

Step 5 To specify an index for this service, continue with the instructions in the section *Setting the Service Index* (on page 7-7).

Step 6 Click **OK**.

The Service Settings dialog box closes.

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

Setting the Service Index

To set a value for the service index:

- Step 1** In the Service Settings dialog box, click the **Advanced** tab.

The Advanced tab of the Service Settings dialog box appears.



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

The service index must be an integer in the range 1 to 499; service index 0 is reserved for the Default Service.

The system automatically assigns a free number for the new service. Only modify this number in cases 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 hierarchy as a child to the service selected in the Parent Service drop-down list.

Editing Services

You can modify the parameters of a service (including services included in the SCAS BB Console installation) at any time.

To add, modify, or delete service elements, see *Managing Service Elements* (on page 7-10).

To edit a service:

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

Step 2 In the Services tab, click  (**Edit Service**).

The Service Settings dialog box appears, open to the General tab.

Step 3 To give a new name to the service, enter a new name in the Name field.

Step 4 To give a new description for the service, enter a new description in the Description field.

Step 5 To change hierarchical settings:

a) Click the **Hierarchy** tab.

The Hierarchy tab of the Service Settings dialog box appears.

b) To set a different parent service: select the desired service from the Parent Service drop-down list.

c) 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 appears in the Global counter used by this service field

d) 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

- Select a value for the counter index from the Counter Index drop-down list

A default value of the counter index is provided by the system; you should not modify this value.

e) To change the subscriber usage counter settings:

- Repeat steps c and d for the subscriber usage counter section of the dialog box

Step 6 To change the service index:

a) In the Service Settings dialog box, click the **Advanced** tab.

The Advanced tab of the Service Settings dialog box appears.

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

The service index must be an integer in the range 1 to 499; service index 0 is reserved for the Default Service.

A default value of the service index is provided by the system; you should not modify this value.

Step 7 Click **OK**.

The Service Settings dialog box closes.


The changes to the service are saved.

Deleting Services

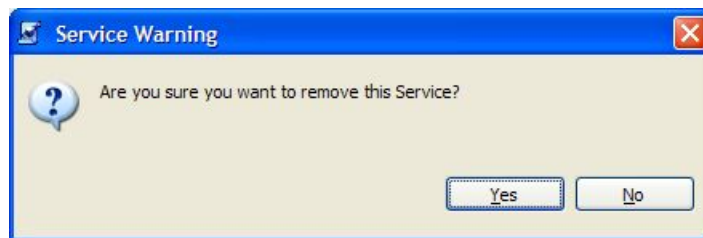
All services can be deleted, including services included in the SCAS BB Console installation. (The Default Service cannot be deleted.)

To delete a service:

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

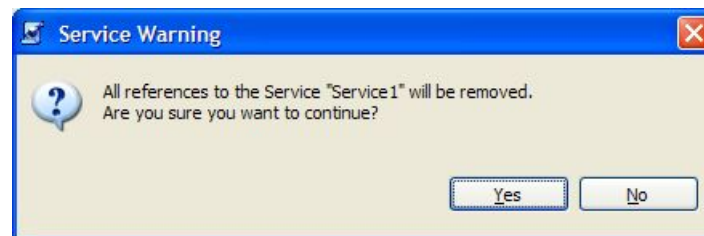
Step 2 In the Services tab, click  (**Remove Service**).

A Service Warning message appears.



Step 3 Click **Yes**.

- If any package has a rule for this service (see *Managing Rules* (on page 9-11)), a second Service Warning message appears



Click **Yes**.

The service is deleted and is no longer displayed in the service hierarchy.

Children of the deleted service are not removed; they are moved up one level in the service hierarchy.

Any rules for the service are also deleted.

Managing 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 on protocols, see *Managing Protocols* (on page 7-20)
- For more information on zones, see *Managing Zones* (on page 7-42)
- For more information on flavors, see *Managing Flavors* (on page 7-48)

A service is a collection of service elements.

- There can be a maximum of 10,000 service elements in a service configuration
- Every service element must be unique

A traffic flow is mapped to a specific 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

Adding Service Elements

When necessary, you can add new service elements to a service. (The most useful service elements are included in the SCAS BB Console installation.) A service may have any number of service elements.



Note

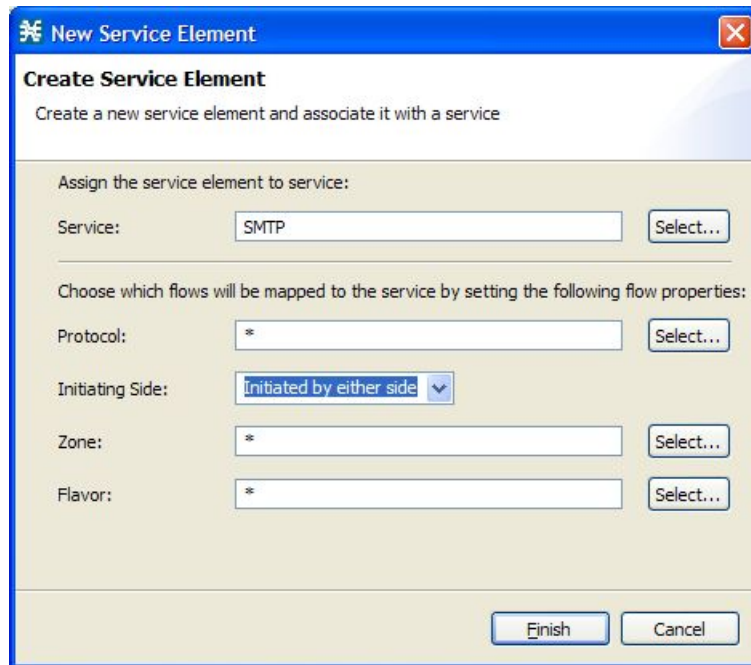
Every service element must be unique; if, at any stage, the new service element is the same as an existing one, an error message is displayed in the dialog box and the Finish button is dimmed - modify the value in at least one field.

To add and define a service element:

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

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

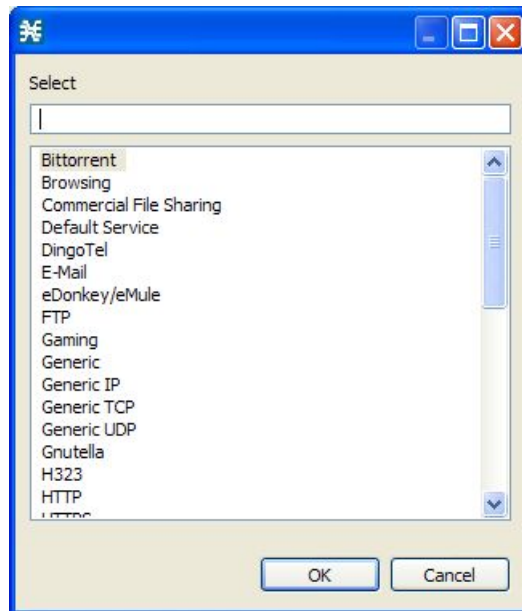
The New Service Element dialog box appears.



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.

The dialog box lists all existing services.



Step 4 Select a service from the list.

Step 5 Click **OK**.

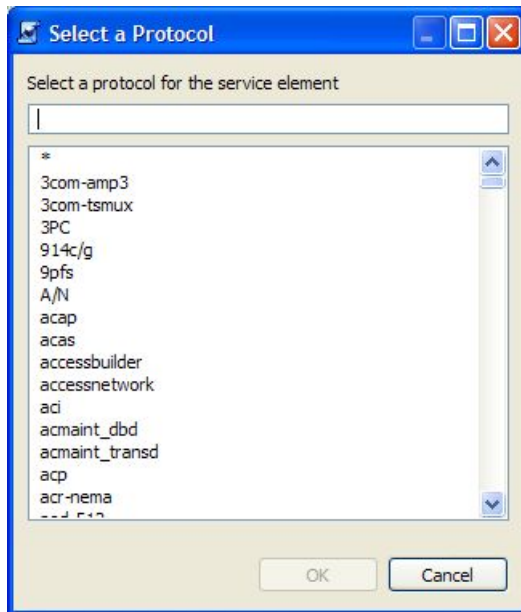
The Select a Service dialog box closes.

The selected service appears in the Service field.

Step 6 Click the **Select** button next to the Protocol field.

The Select a Protocol dialog box appears.

The dialog box includes a list of all available protocols.



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.

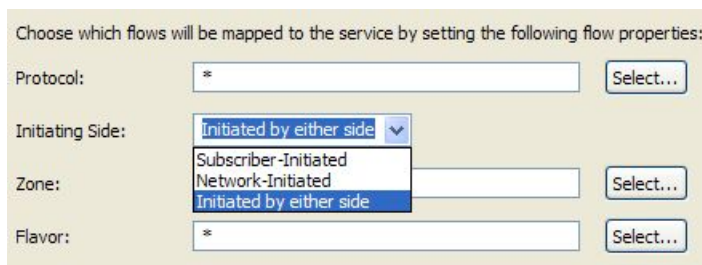
The default value (an asterisk, *) means that no protocol checking is performed when testing if a flow maps to this service element.

Step 8 Click **OK**.

The Select a Protocol dialog box closes.

The selected protocol appears in the Protocol field.

Step 9 In the Initiating Side field, click the drop-down arrow.



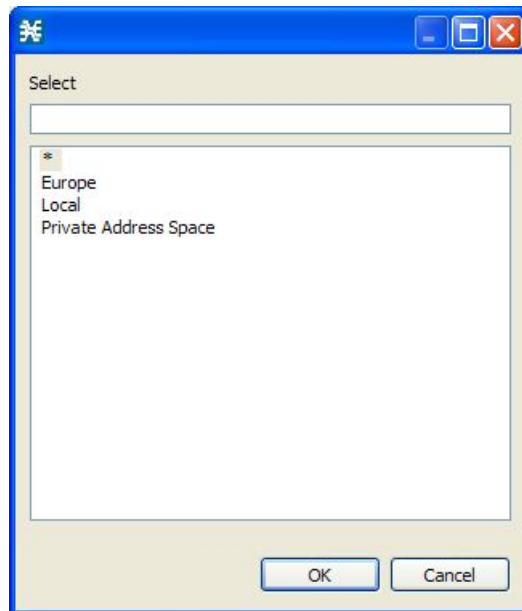
Step 10 Select the appropriate initiating side from the drop-down list. The following options are available:

- **Subscriber-Initiated**—Transactions that are initiated at the subscriber side towards (a server at) the network side
- **Network-Initiated**—Transactions that are initiated at the network side towards (a server at) the subscriber side
- **Initiated by either side**—This is the default value

Step 11 Click the **Select** button next to the Zone field.

The Select a Zone dialog box appears.

The dialog box includes a list of all available zones.



Step 12 Select a zone from the list.

The default value (an asterisk, *) means that no zone checking is performed when testing if a flow maps to this service element.

Step 13 Click **OK**.

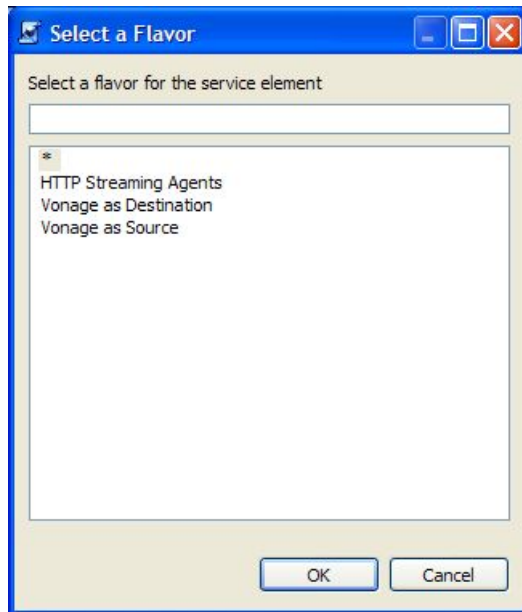
The Select a Zone dialog box closes.

The selected zone appears in the Zone field.

Step 14 Click the **Select** button next to the Flavor field.

The Select a Flavor dialog box appears.

The dialog box includes a list of all available flavors.



Step 15 Select a flavor from the list.

The default value (an asterisk, *) means that no flavor checking is performed when testing if a flow maps to this service element.

Step 16 Click **OK**.

The Select a Flavor dialog box closes.

The selected flavor appears in the Flavor field.

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.


Duplicating Service Elements

You can duplicate an existing service element. This is a useful way to add a new service element that is 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 - modify the value in at least one field.

To duplicate a service element:

- Step 1** In the Services tab, select a service from the service tree.
A list of associated service elements appears in the Service Elements pane.
- Step 2** In the Service Elements pane, select a service element to duplicate.
- Step 3** In the Services Elements pane, click  (**Duplicate Services Element**).

Step 4 The Copy Service Element dialog box appears.

Step 5 Modify the service element as required (see *Editing Service Elements* (on page 7-16)).

You must change the value in at least one field before you can save the new service element.

Editing Service Elements

All service elements can be modified, including service elements included in the SCAS BB 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 - modify the value in at least one field.

To edit a service element:

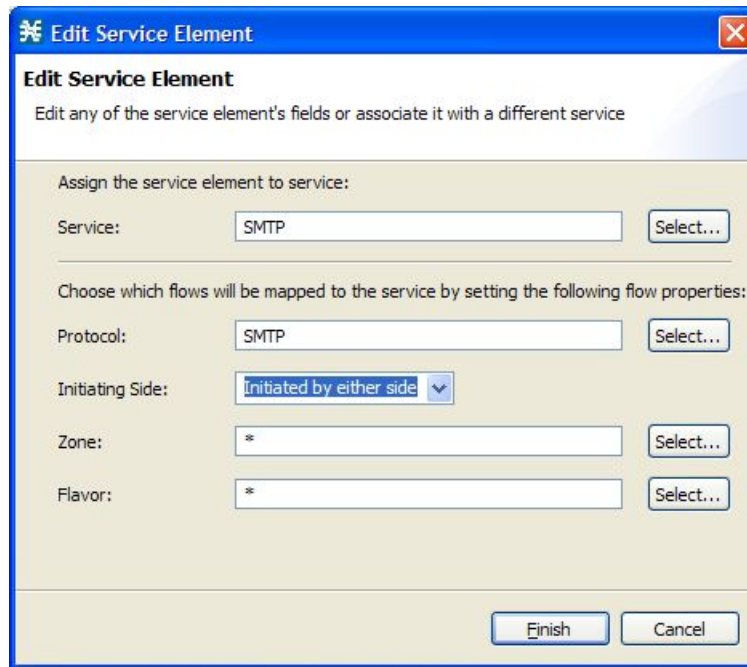
Step 1 In the Services tab, select a service from the service tree.

A list of associated service elements appears in the Service Elements pane.

Step 2 In the Service Elements pane, select a service element to edit.

Step 3 In the Services Elements pane, click  (**Edit Service Element**).

The Edit Service Elements 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.

The dialog box lists all existing services.

Step 5 Select a service from the list.

Step 6 Click **OK**.

The Select a Service dialog box closes.

The selected service appears in the Service field.

Step 7 To change the protocol of this service element, click the **Select** button next to the Protocol field.

The Select a Protocol dialog box appears.

The dialog box includes a list of all available 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.

The default value (an asterisk, *) means that no protocol checking is performed when testing if a flow maps to this service element.

Step 9 Click **OK**.

The Select a Protocol dialog box closes.

The selected protocol appears in the Protocol field.

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 that are initiated at the subscriber side towards (a server at) the network side
- **Network-Initiated**—Transactions that are initiated at the network side towards (a server at) the subscriber side
- **Initiated by either side**—This is the default value

Step 12 To change the zone of this service element, click the **Select** button next to the Zone field.

The Select a Zone dialog box appears.

The dialog box includes a list of all available zones.

Step 13 Select a zone from the list.

The default value (an asterisk, *) means that no zone checking is performed when testing if a flow maps to this service element.

Step 14 Click **OK**.

The Select a Zone dialog box closes.

The selected zone appears in the Zone field.

Step 15 To change the flavor of this service element, click the **Select** button next to the Flavor field.

The Select a Flavor dialog box appears.

The dialog box includes a list of all available flavors.

Step 16 Select a flavor from the list.

The default value (an asterisk, *) means that no flavor checking is performed when testing if a flow maps to this service element.

Step 17 Click **OK**.

The Select a Flavor dialog box closes.

The selected flavor appears in the Flavor field.

Step 18 Click **Finish**.

The Edit Service Element dialog box closes.


The changes to the service element are saved.

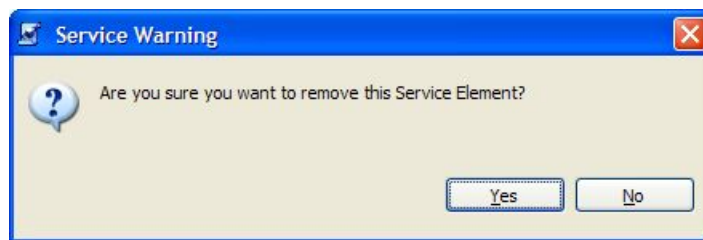
The changes to the service element appear in the service element list in the Service Elements pane.

Deleting Service Elements

All service elements can be deleted, including service elements included in the SCAS BB Console installation.

To delete a service element:

-
- Step 1** In the Services tab, select a service from the service tree.
A list of associated service elements appears 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  (**Remove 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.
-

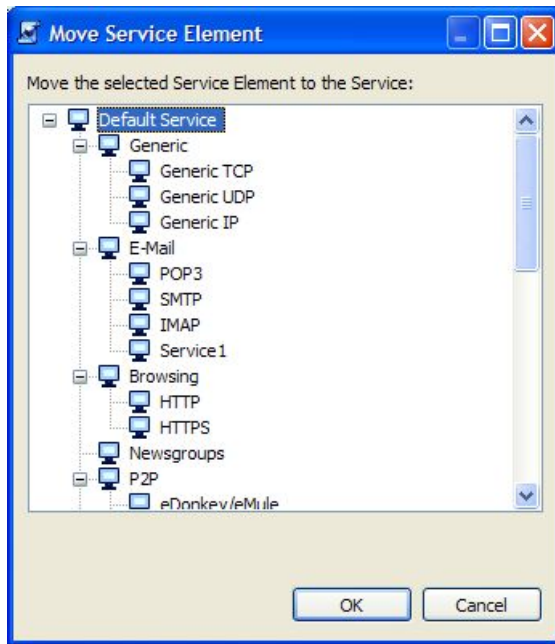
Moving Service Elements

You can move an existing service element from one service to a different service.

To move a service element:

-
- Step 1** In the Services hierarchy, select a service.
A list of associated service elements appears in the Service Elements pane.
- Step 2** In the Service Elements pane, select a service element to move.
- Step 3** In the Service Elements pane, click  (**Move Service Element to Another Service**).
The Move Service Element dialog box appears.

The dialog box includes 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* (on page 7-10)).

You can add new protocols (for example, to classify a new gaming protocol that uses a specific port) and edit or delete existing ones.

SCA BB supports many commercial and common protocols. For a complete list of protocols, see 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 *Adding Dynamic Signatures to the Service Configuration* (on page 7-34).)

Protocols have the following limitations:

- There can be a maximum of 10,000 protocols in a service configuration
- Every protocol element must be unique

Viewing Protocols

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

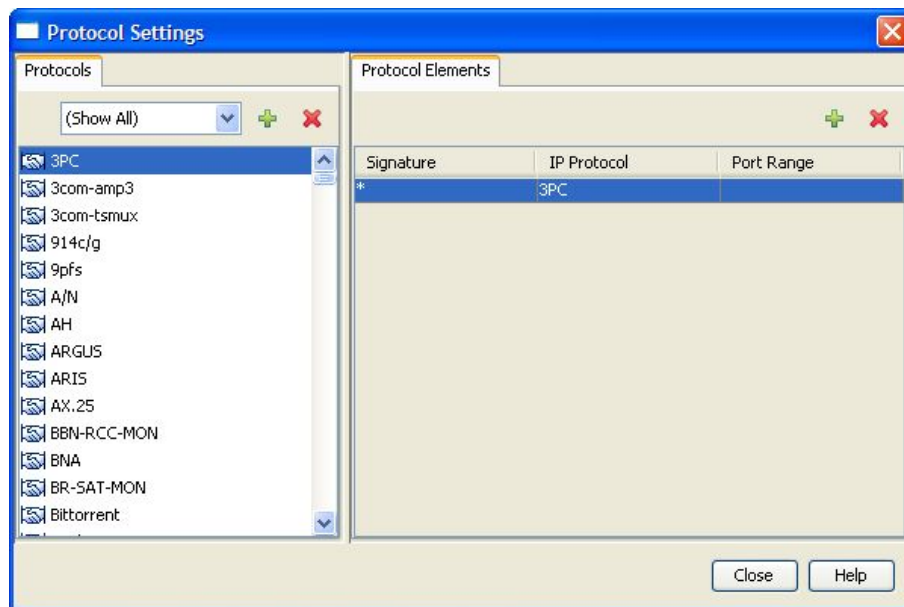
The protocols are listed in ASCII sort order (that is, 0 ... 9, A ... Z, a ... z).

Protocol elements are not sorted; they are listed in the order in which they are added to the protocol.

To view a list of all protocols:

Step 1 From the **Configuration** menu, choose **Protocols**.

The Protocol Settings dialog box appears.

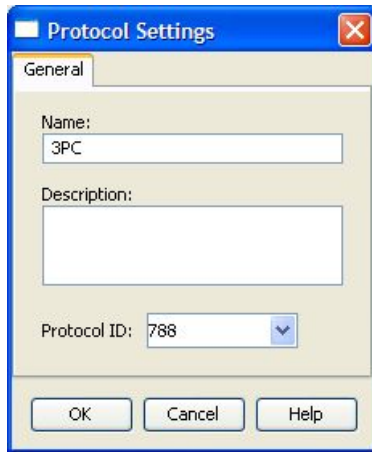


Step 2 The Protocols tab displays a list of existing protocols.

Step 3 To view the description and ID of a protocol:

- a) Double-click on a protocol.

The Protocol Settings dialog box appears, displaying the protocol name, description, and ID.



b) Click **Cancel**.

c) The Protocol Settings dialog box closes.

Step 4 Click on a protocol in the list to display a list of protocol elements.

The protocol elements are displayed in the Protocol Elements tab.

Step 5 Click **Close**.

The Protocol Settings dialog box closes.

Filtering the Protocols View

You can filter the protocols by type, so that the Protocol List pane displays only the selected type of protocol.

Protocols are divided into four groups:

- **Generic Protocols**—Generic IP, Genetic TCP, and Generic UDP protocols, used for transactions that are not specifically mapped to a protocol by one of the following, more specific protocol types.
- **IP Protocols**—Non-TCP/UDP protocols (such as ICMP), identified according to the IP protocol number of the transaction.
- **Port-Based Protocols**—TCP and UDP protocols that are 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 Layer7 application signature. This group includes the most common protocols, such as HTTP and FTP, as well as a large group of popular P2P protocols.



Note Some protocols belong to more than one category.

To filter the protocol list:

Step 1 From the **Configuration** menu, choose **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 List pane.

Step 3 Click **Close**.

The Protocol Settings dialog box closes.

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.

Adding Protocols

When necessary, you can add new protocols to a service configuration.

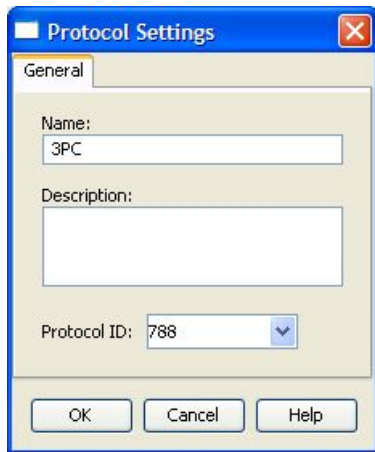
To add a new protocol:

Step 1 From the **Configuration** menu, choose **Protocols**.

The Protocol Settings dialog box appears.

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

The Protocol Settings dialog box appears.



Step 3 (Optional) In the Name field, enter a unique name for the new protocol.

The default name for the protocol can be used; it is recommended that you enter a meaningful name.

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*.

The value of the protocol ID is supplied automatically by the system; you should not modify this field.

Step 5 Click **OK**.

The Protocol Settings dialog box closes.

The new protocol appears in the Protocols tab. You can now add protocol elements, *see Adding Protocol Elements* (on page 7-27).

Editing Protocols

You can modify the parameters of a protocol (including protocols included in the SCAS BB Console installation) at any time.

To add, modify, or delete protocol elements, *see Managing Protocol Elements* (on page 7-26).

To edit a protocol:

Step 1 From the **Configuration** menu, choose **Protocols**.

The Protocol Settings dialog box appears.

- Step 2** In the Protocols tab, double-click on a protocol.
The Protocol Settings dialog box appears.



- Step 3** Modify fields in the 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*.

The value of the protocol ID is supplied automatically by the system; you should 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.

Deleting Protocols


All protocols can be deleted, including protocols included in the SCAS BB Console installation.

To delete a protocol

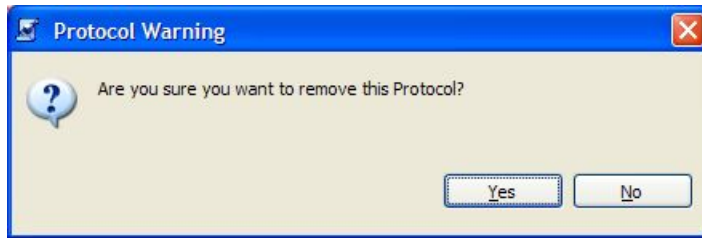
- Step 1** From the **Configuration** menu, choose **Protocols**.

The Protocol Settings dialog box appears.

- Step 2** In the Protocols tab, select a Protocol.

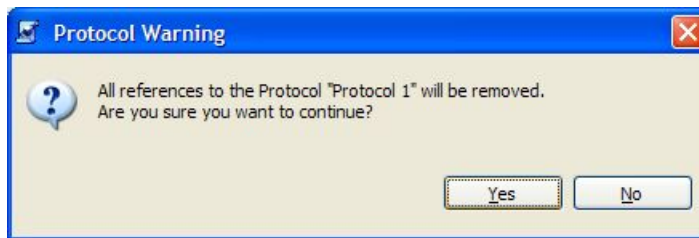
Step 3 In the Protocols tab, click  (**Delete Protocol**).

A Protocol Warning message appears.



Step 4 Click **Yes**.

- If any service element maps the selected protocol to a service (see *Managing Service Elements* (on page 7-10)), 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

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.

A protocol is a collection of protocol elements.

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
- The destination port is within the specified port range of the protocol element (applicable only when the IP protocol is TCP or UDP)
- The protocol element is the most specific protocol element satisfying the first three criteria

Every protocol element must be unique.

Adding Protocol Elements

You can add protocol elements to any protocol. A protocol may have any number of protocol elements.



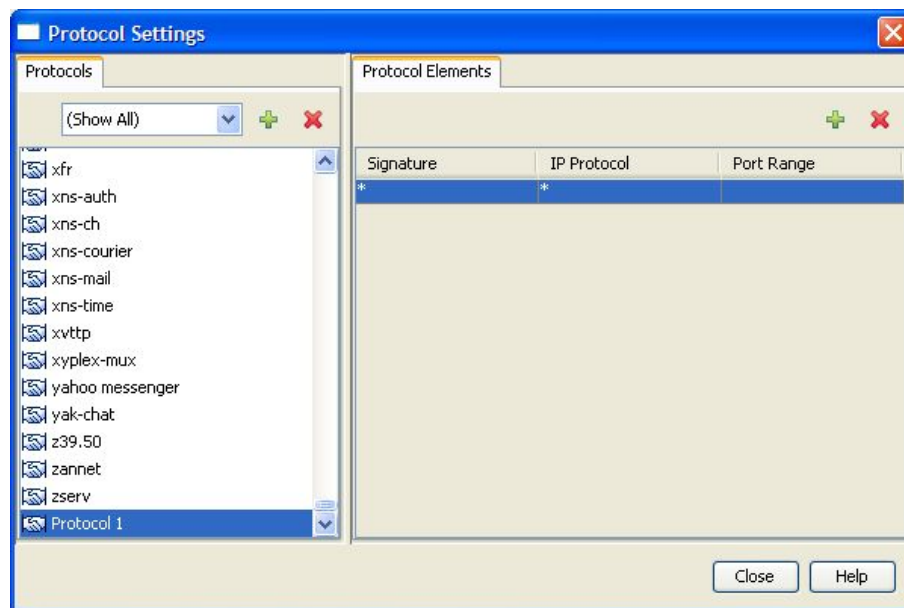
Note When you set the parameters of the protocol element, the values of the parameters are saved as you enter them.

To add and define a protocol element:

- Step 1** From the **Configuration** menu, choose **Protocols**.
The Protocol Settings dialog box appears.
- Step 2** Select a protocol in the Protocols tab.
- Step 3** In the Protocol Elements tab, click **+** (**Add Protocol Element**).

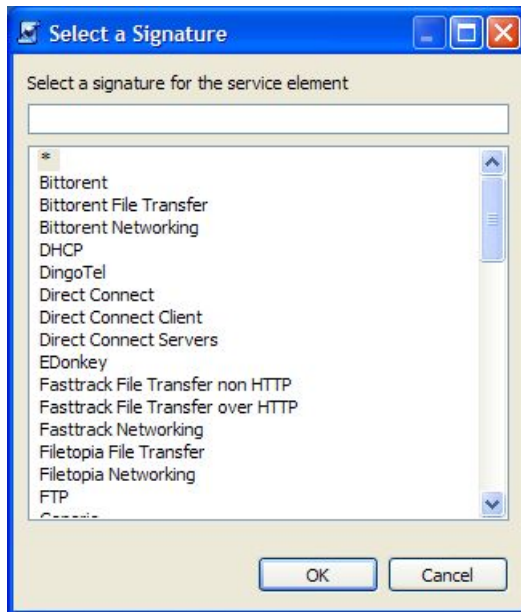
A protocol element is added to the protocol.

A new row, representing the protocol element, is added to the protocol element list in the Port Number tab.



- Step 4** (Optional) 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 Choose a signature from the list.

The default value (an asterisk, *) means that no signature checking is performed when testing if a flow maps to this protocol element.

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 it also matches the IP protocol and port range of the protocol element).

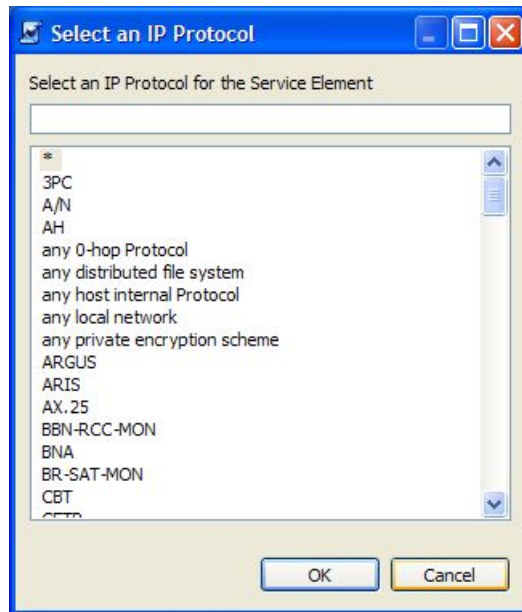
Step 6 Click **OK**.

The Select a Signature dialog box closes.

The selected signature appears in the Signature cell.

Step 7 (Optional) 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 Choose an IP protocol from the list.

The default value (an asterisk, *) means that no IP protocol checking is performed when testing if a flow maps to this protocol element.

The selected IP protocol appears in the IP Protocol cell.

Step 9 Click **OK**.

The Select an IP Protocol dialog box closes

Step 10 (Optional) In the Port Range cell, enter a port or range of ports. (Use a hyphen between the port range bottom and top bounds (inclusive).)

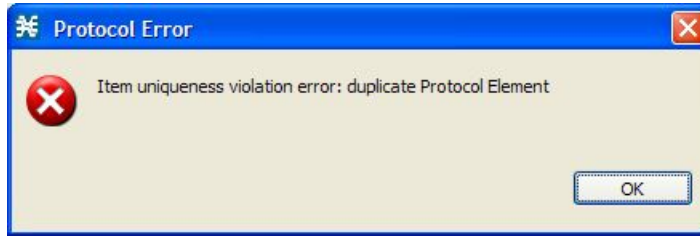
Specifying a port range is only possible when the specified IP protocol is either TCP or UDP (or undefined, taking the wild-card value, *).

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

The protocol element is now defined.

Step 11 Click **Close**.

- a) If the protocol element that you have defined is not unique in this service configuration, a Protocol Error message appears:



- b) Click **OK**.
- c) Modify or delete the protocol element.
- d) Click **Close**.

The Protocol Settings dialog box closes.

Editing Protocol Elements

All protocol elements can be modified, including protocol elements included in the SCAS BB Console installation.



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

To edit a protocol element:

- Step 1** From the **Configuration** menu, choose **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** 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**.

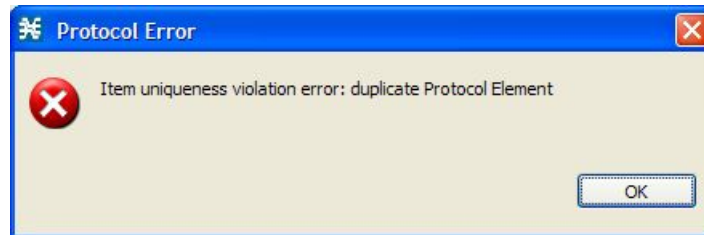
The Select an IP Protocol dialog box closes.

Step 10 In the Port Range cell, enter a port or range of ports.

Changes to the protocol element are saved as you make them.

Step 11 Click **Close**.

- a) If the protocol element that you have modified is not unique in this service configuration, a Protocol Error message appears:



- b) Click **OK**.
c) Modify or delete the protocol element.
d) Click **Close**.

The Protocol Settings dialog box closes.

Deleting Protocol Elements

All protocol elements can be deleted, including protocol elements included in the SCAS BB Console installation.


To delete a protocol element:

Step 1 From the **Configuration** menu, choose **Protocols**.

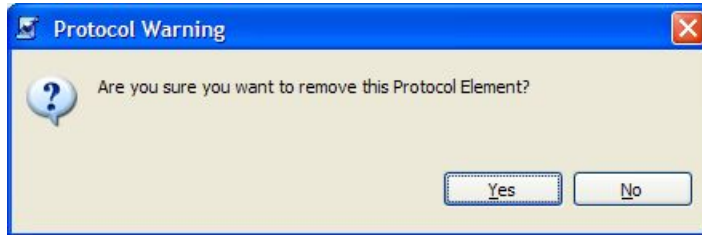
The Protocol Settings dialog box appears.

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 Protocol Signatures: 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 where a new protocol is released and a customer would like to be able to classify its traffic (for example, a new P2P protocol in a P2P-Control solution).

- Installing new signatures to an active service configuration is described in *Installing Protocol Packs* (on page 4-8)
- Creating and modifying signatures is described in *Using the Signature Editor* (on page 12-1)
- Using servconf, the *SCA BB* Server Configuration Utility, to apply signatures is described in *The Cisco Service Control Application for Broadband Service Configuration Utility* (on page 13-1)

Dynamic Signature Script Files

Dynamic signatures are provided in special Dynamic Signatures Script (DSS) files which can be added to a service configuration using the SCAS BB Console or the Service Configuration API. Once a DSS file is loaded into a service configuration, the new protocols it describes appear in the protocol list, can be added to services as required, and 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, while 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 importing 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"

**Note**

When the import of a DSS is completed, you should associate the newly added protocols with services.

Cisco may release an improved version of a previously released DSS. The improved DSS may add new protocols, add new signatures, or update previously defined signatures. To update the service configuration with the new DSS, perform a normal import DSS procedure as explained in the following section. The import procedure preserves all service and protocol settings.

DSS files are periodically released by Cisco or its partners in accordance with customer requirements and market needs. You can create your own DSS files or modify the Cisco release DSS file using the Signature Editor tool (see *Managing DSS Files* (on page 12-1)).

Viewing Current Dynamic Signatures Information

To view information about the current dynamic signatures:

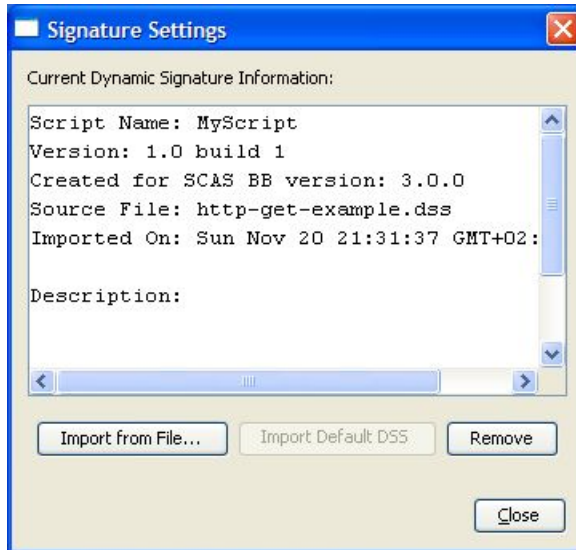
Step 1 From the **Configuration** menu, choose **Signatures**.

The Signature Settings dialog box appears.

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



- If a DSS file was imported into the current service configuration, the Signature Settings dialog box displays information about the current dynamic signatures and the DSS file from which they were imported.



Step 2 Click **Close**.

The Signature Settings dialog box closes.

Adding Dynamic Signatures to the Service Configuration

You can import signatures into a service configuration from a DSS file provided by Cisco or one of its partners, or from a DSS file that you have created or modified using the Signature Editor tool (see *Managing DSS Files* (on page 12-1)).



Note Instead of using this option, it is recommended that you import the latest default DSS file (see *Importing Dynamic Signatures from the Default DSS File* (on page 7-40)) when creating or modifying a service configuration.

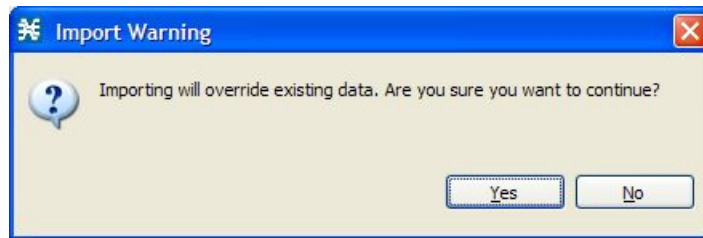
To import a dynamic signature script:

Step 1 From the **Configuration** menu, choose **Signatures**.

The Signature Settings dialog box appears.

Step 2 Click **Import from File**.

An Import Warning message appears.



Step 3 Click **Yes**.

The Import from file dialog box appears.

Step 4 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 are displayed in the Signature Settings dialog box.

Step 5 Click **Close**.

The Signature Settings dialog box closes.

Removing Dynamic Signatures

You can remove the installed dynamic signatures from the service configuration.



Note The DSS file is not deleted.

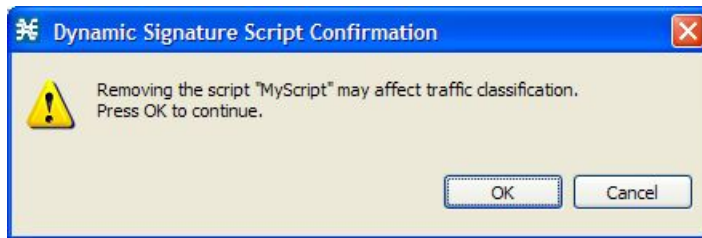
To remove the current dynamic signatures information:

Step 1 From the **Configuration** menu, choose **Signatures**.

The Signature Settings dialog box appears.

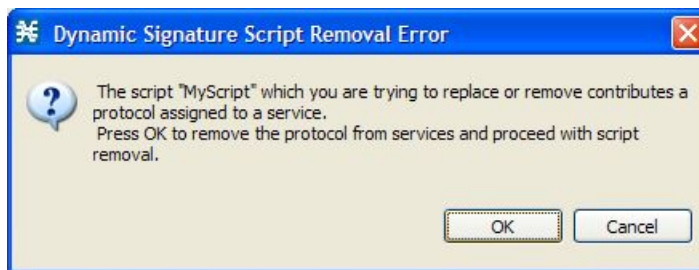
Step 2 In the Signature Settings dialog box, click **Remove**.

A Dynamic Signature Script Confirmation message appears.



Step 3 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 4 Click **Close**.

The Signature Settings dialog box closes.

The Default DSS File

Offline service configurations (stored as PQB files on the workstation) should be updated whenever a protocol pack becomes available from Cisco or one of its partners. The protocol pack is provided as either an SPQI or DSS file. (There is a difference in behavior when applying the protocol pack to an SCE platform (see *SPQI Files* (on page 4-9)).)

Updates should be offered automatically to every service configuration created or edited at the workstation, or applied from the workstation to the SCE platform. Making the latest update available is achieved by installing the most recent DSS or SPQI file as the default DSS file. The file can be installed on the workstation either from the SCAS BB Console or by using the *SCA BB Signature Configuration Utility* (on page 13-4).

- The default DSS file is automatically offered for import when any service configuration operation (such as creating a new service configuration or editing an existing service configuration) is performed from the SCAS BB Console on a service configuration that has not yet been updated.
- The default DSS file is imported, by default, when any service configuration operation (such as applying an existing service configuration) is performed using *servconf*, the *Cisco Service Control Application for Broadband Service Configuration Utility* (on page 13-1). 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 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 *Editing DSS Files* (on page 12-12)) to add signatures of new protocols until they become available from Cisco.

Whenever a new protocol pack becomes available, install it as the default DSS file; there is no need to uninstall the current default DSS file, it will be overwritten by the new protocol pack.

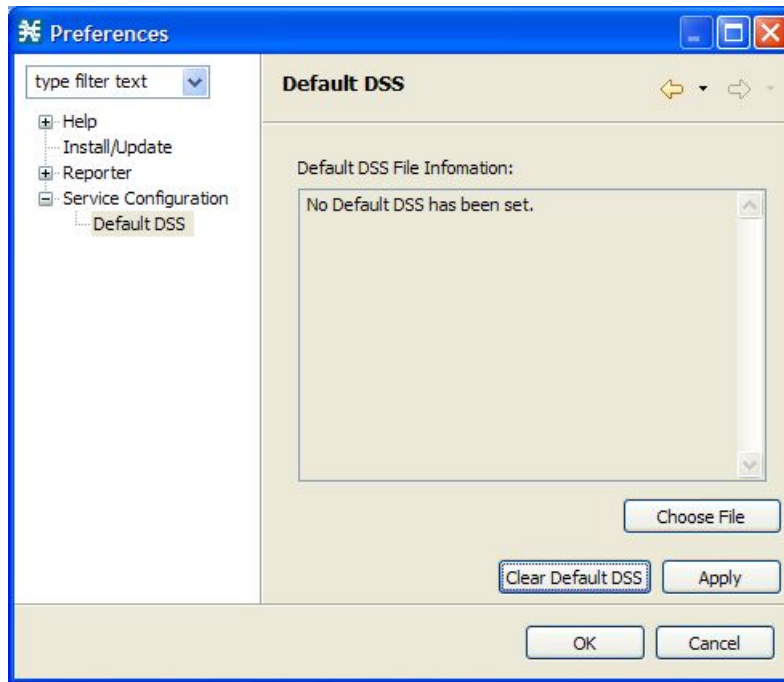
To install a protocol pack as the default DSS file:

Step 1 From the **Windows** menu, choose **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 appears in the right pane of the dialog box.



Step 3 Click **Choose File**.

An Open dialog box appears.

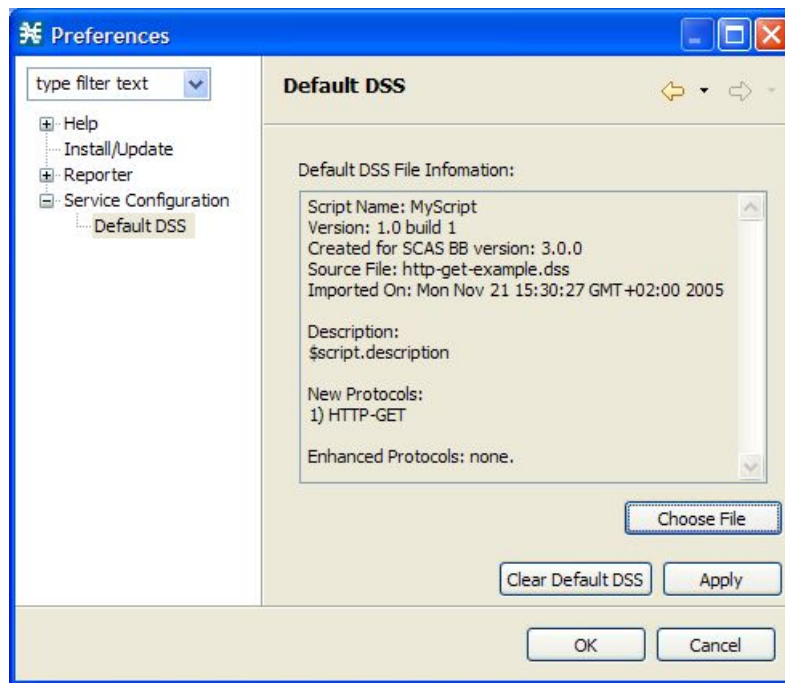
Step 4 From the Files of type drop-down list, select the file type of the protocol pack.

Step 5 Browse to the protocol pack.

Step 6 Click **Open**.

The Open dialog box closes.

Information about the default DSS file appears in the Default DSS pane of the Preferences dialog box.



Step 7 Click **OK**.

The DSS file is copied to *C:\Documents and Settings\\.profile\default3.0.0.dss* as the default DSS file.

The Preferences dialog box closes.

To uninstall the default DSS file:

Step 1 From the **Windows** menu, choose **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 appears in the right pane of the dialog box.

Step 3 Click **Clear Default DSS**.

The default DSS file, *C:\Documents and Settings\\.profile\default3.0.0.dss*, is deleted.

All information is deleted from the Default DSS pane.

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 can import the dynamic signatures from the file when you create a new service configuration or open an existing service configuration that has not imported the signatures. Alternatively, you can manually import the dynamic signatures at any time.

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 Do one of the following:

- Click **Yes** to import the default DSS file
 - Click **No** to continue without importing the default DSS file
-

To import the default DSS file manually:

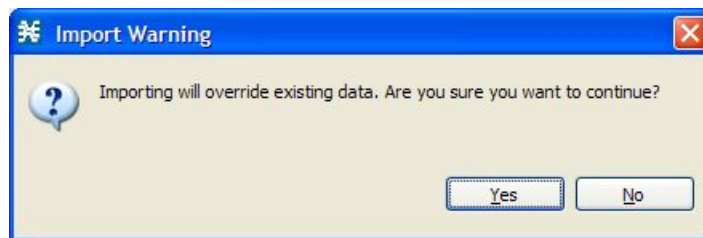
Step 1 From the **Configuration** menu, choose **Signatures**.

The Signature Settings dialog box appears with the Import Default DSS button enabled.



Step 2 Click **Import Default DSS**.

An Import Warning message appears.



Step 3 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 are displayed in the Signature Settings dialog box.

Step 4 Click **Close**.

The Signature Settings dialog box closes.

Managing Zones

A *zone* is a collection of destination IP addresses. Each zone is defined by the user; usually the IP addresses in one zone will be related in some way.

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

Zones have the following limitations:

- There can be a maximum of 10,000 zone items in a service configuration
- Every zone item must be unique

Viewing Zones

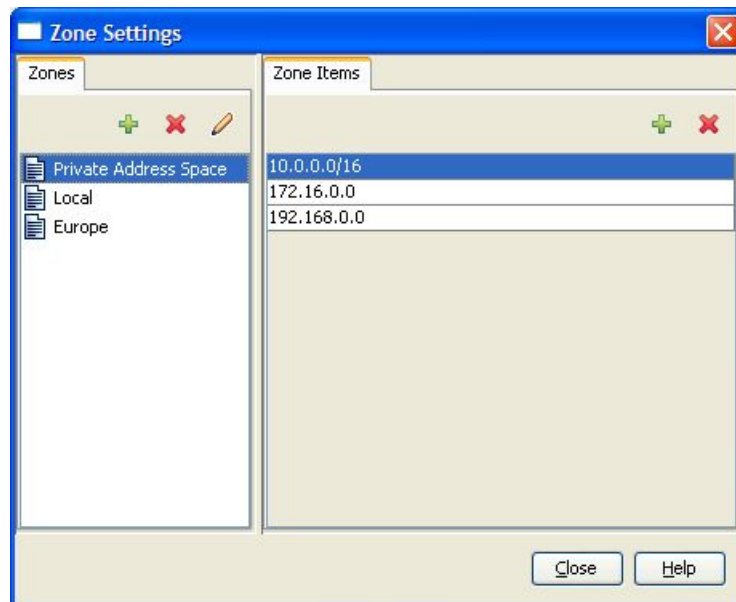
You can view a list of all existing zones and their associated zone items.

To view a list of all zones:

Step 1 From the **Configuration** menu, choose **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 on 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.

Adding Zones

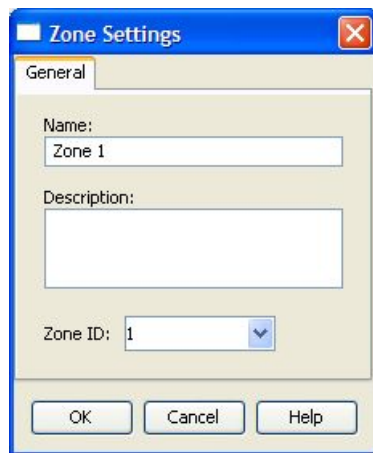
To add a zone to a service configuration:

- Step 1** From the **Configuration** menu, choose **Zones**.

The Zone Settings dialog box appears.

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

The Zone Settings dialog box appears.



- Step 3** (Optional) In the Name field, enter a unique name for the new zone.

The default name for the zone can be used; it is recommended that you enter a meaningful name.

- 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.

The value of the zone ID is supplied automatically by the system; you should not modify this field.

- Step 5** Click **OK**.

The Zone Settings dialog box closes.

The new zone appears in the Zones tab. You can now add zone items, see *Adding Zone Items* (on page 7-45).

Editing Zones

You can modify zone parameters at any time.

To add, modify, or delete zone items, see *Managing Zone Items* (on page 7-45).

To edit a zone:

Step 1 From the **Configuration** menu, choose **Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, from the zone list, select a zone.

Step 3 In the Zones tab, 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

The value of the zone ID is supplied automatically by the system; you should 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.

Deleting Zones


You can delete any or all zones.

To delete a zone:

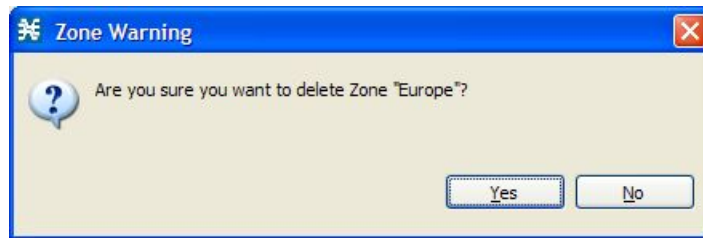
Step 1 From the **Configuration** menu, choose **Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, from the zone list, select a zone.

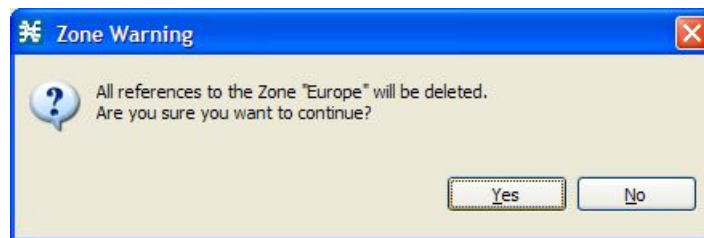
Step 3 In the Zones tab, click  (**Delete Zone**).

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 item* is an IP address or a range of IP addresses.

A zone is a collection of related zone items.

- There can be a maximum of 10,000 zone items in a service configuration
- Every zone item must be unique

Adding 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).

To add zone items to a zone:

Step 1 From the **Configuration** menu, choose **Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, from the zone list, select a zone.

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

A new line is added to the Zone Items table.

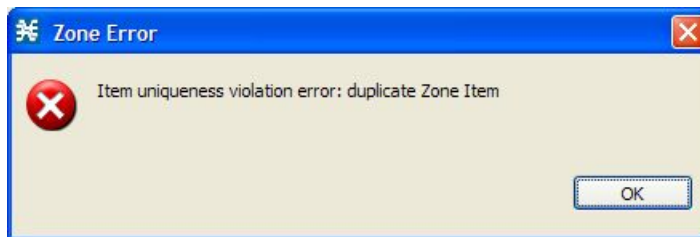
Step 4 Double-click the new list item and enter a valid value.

Valid values are single IP addresses (for example, 63.111.106.7) or a range of IP addresses (for example, 194.90.12.0/24).

Step 5 Repeat steps 3 and 4 for other IP addresses that are to be part of this zone.

Step 6 Click **Close**.

- a) If the zone item that you have defined is not unique in this service configuration, a Zone Error message appears:



- b) Click **OK**.

- c) Modify or delete the zone item.

- d) Click **Close**.

The Zone Settings dialog box closes.

Editing Zone Items

To edit a zone item:

Step 1 From the **Configuration** menu, choose **Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, from the zone list, select a zone.

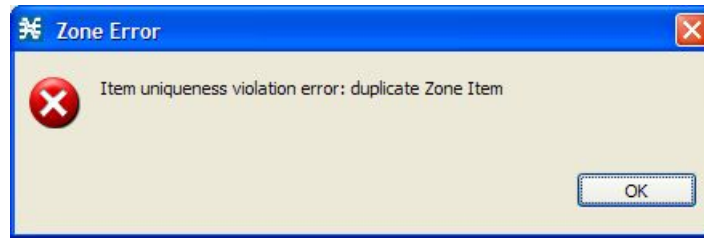
Step 3 In the Zone Items tab, double-click on a zone item.

Step 4 Enter a new value for the zone item.

Valid values are single IP addresses (for example, 63.111.106.7) or a range of IP addresses (for example, 194.90.12.0/24).

Step 5 Click **Close**.

- a) If the zone item that you have modified is not unique in this service configuration, a Zone Error message appears:



- b) Click **OK**.
- c) Modify or delete the zone item.
- d) Click **Close**.

The Zone Settings dialog box closes.

Deleting Zone Items


To delete a zone item:

- Step 1** From the **Configuration** menu, choose **Zones**.

The Zone Settings dialog box appears.

- Step 2** In the Zones tab, from the zone list, select a zone.

- Step 3** In the Zone Items tab, from the zone item list, 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 Flavors

Flavors are advanced classification elements that are used to classify network sessions.

Flavors are based on specific L7 properties. For instance, 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.

Flavors have the following limitations:

- There is a maximum number of flavor items for each flavor type (see *Maximum Number of Flavor Items per Flavor Type* (on page 7-52))
- For each flavor type, every flavor item must be unique

Flavor Types and Parameters

The following table lists available flavor types:

Flavor Type	Applicable for protocol	Valid Values
User Agent	HTTP RTSP	Prefix string
URL	HTTP	<host suffix, path prefix, path suffix, URL params prefix> <ul style="list-style-type: none"> • Host—From the beginning of the URL till the first '/' • Path—The section from the first '/' to the '?' • URL params—Any string following the '?' (It is not required to start the params prefix with '?')
Host Name	RTSP SMTP	Host suffix
SIP Source Domain	SIP	Host suffix
SIP Destination Domain	SIP	Host suffix
Composite Flavor (Composite Flavors are pairs of two defined flavors)	HTTP RTSP SIP	<user agent flavor, URL flavor> <user agent flavor, host name flavor> <SIP source domain, SIP destination domain>

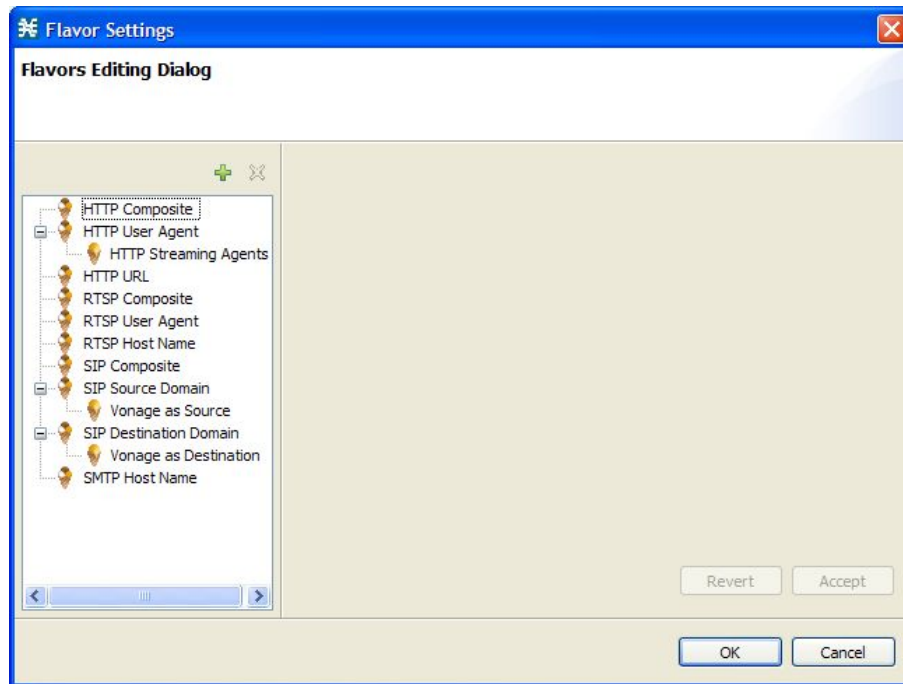
Viewing Flavors

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

To view a list of all flavors:

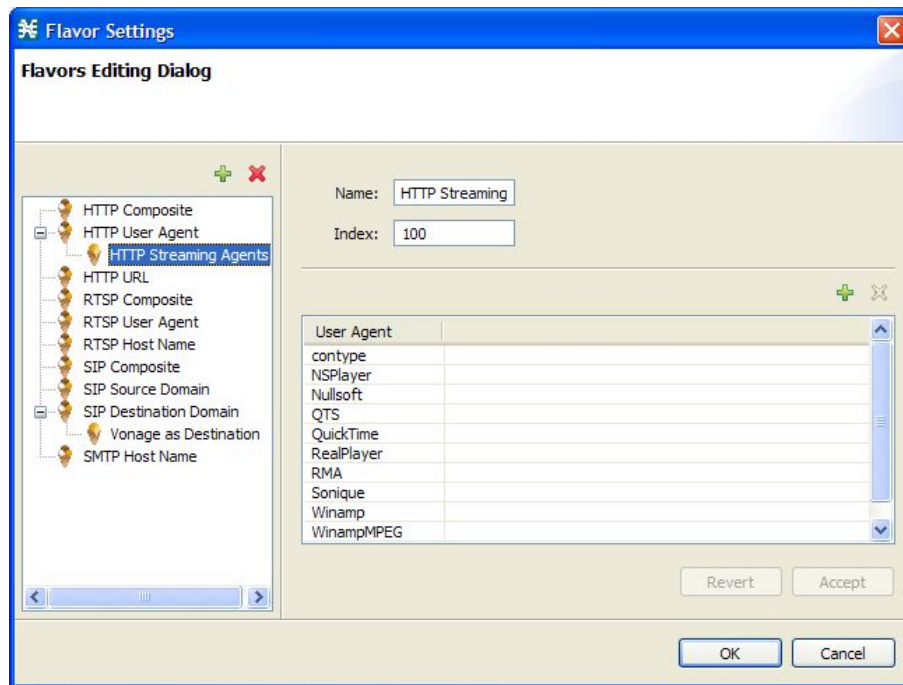
Step 1 From the **Configuration** menu, choose **Flavors**.

The Flavor Settings dialog box appears.



The left-hand area displays a tree showing all flavors of each flavor type.

Step 2 Click on a flavor in the list to display its flavor items.



The flavor items are displayed in the right-hand area.

Step 3 Click **OK**.

The Flavor Settings dialog box closes.

Adding Flavors

Any number of flavors can be added to a service configuration.

To add a flavor:

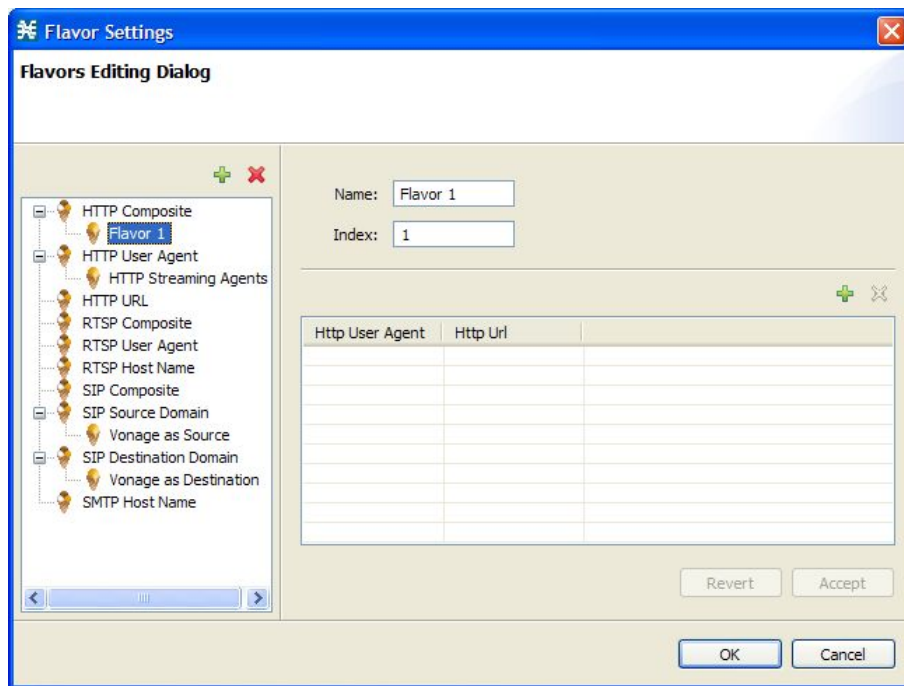
Step 1 From the **Configuration** menu, choose **Flavors**.

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.

Step 5 In the Index field, enter an integer.

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 *Adding Flavor Items* (on page 7-53).

Editing Flavors

You can modify flavor parameters at any time.

To add, modify, or delete flavor items, see *Managing Flavor Items* (on page 7-52).

To edit a flavor:

Step 1 From the **Configuration** menu, choose **Flavors**.

The Flavor Settings dialog box appears.

Step 2 In the flavor list, from the flavor list, select a flavor.

Step 3 In the flavor list, click on a flavor.

The name and index of the flavor (and its flavor items) are displayed in the right-hand area.

Step 4 Modify fields in the dialog box:

- In the Name field, enter a new name for the flavor
- In the Index field, enter a new index for the flavor

The flavor index must be a positive integer in the range 1 to 32767

Step 5 Click **OK**.

The Flavor Settings dialog box closes.

Deleting Flavors

You can delete any or all flavors.

To delete a flavor:

Step 1 From the **Configuration** menu, choose **Flavors**.

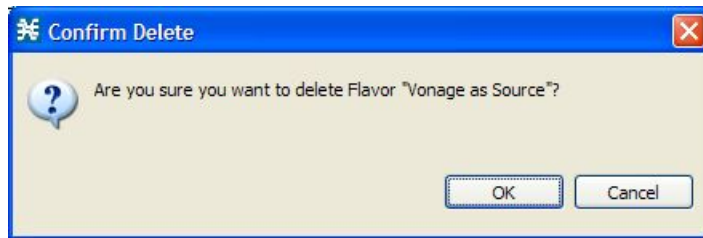
The Flavor Settings dialog box appears.

Step 2 In the flavor list, right-click on a flavor.

A short-cut menu appears.

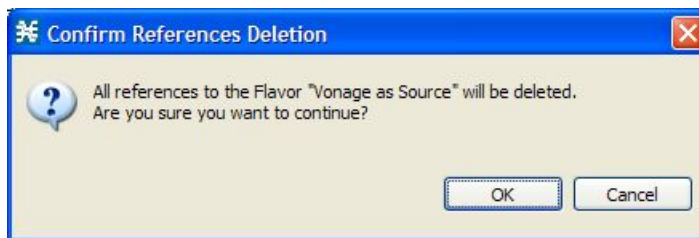
Step 3 Click  **Delete**.

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 list.

Step 5 Click **Close**.

The Flavor Settings dialog box closes.

Managing 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* (on page 7-48)).

A flavor is a collection of related flavor items.

- There is a maximum number of flavor items for each flavor type (see the table in the following section) per service configuration
- For each flavor type, every flavor item must be unique

Maximum Number of Flavor Items per Flavor Type

The following table lists the maximum number of flavor items for each flavor type:

Flavor Type	Maximum No. of Flavor Items
HTTP Composite	10,000

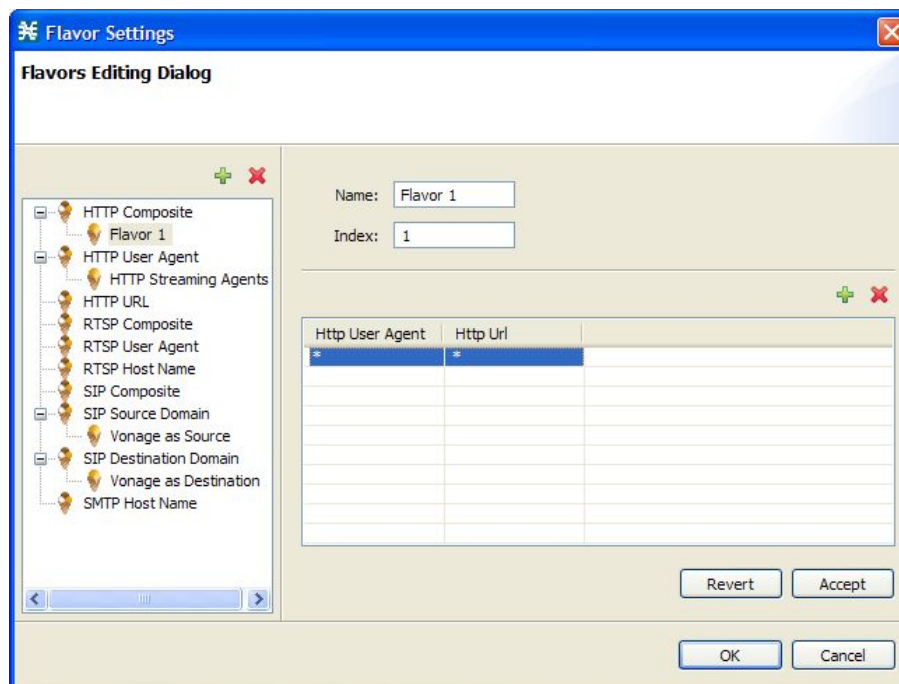
HTTP User Agent	128
HTTP URL	100,000
RTSP Composite	10,000
RTSP User Agent	128
RTSP Host Name	10,000
SIP Composite	10,000
SIP Source Domain	128
SIP Destination Domain	128
SMTP Host Name	10,000

Adding 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).

To add flavor items to a flavor:

- Step 1** From the **Configuration** menu, choose **Flavors**.
The Flavor Settings dialog box appears.
- Step 2** In the flavor tree, click on 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* (on page 7-48)).

The new flavor item has a default value of all wild cards (asterisks).

Step 4 For each cell of the new flavor item, click on the asterisk and then enter an appropriate value.

Step 5 For the composite flavors, and for HTTP Content Category flavor, a Browse button is displayed when clicking on the asterisk:

a) Click the **Browse** button.

A Select dialog appears, displaying all valid values for the parameter.

b) Select an appropriate value from the list.

c) Click **OK**.

The Select dialog closes.

The selected value is displayed in the cell.

Step 6 Repeat steps 3 to 6 for other flavor items, as required.

Step 7 Click **OK**.

The Flavor Settings dialog box closes.

Editing Flavor Items

To edit a flavor item:

Step 1 From the **Configuration** menu, choose **Flavors**.

The Flavor Settings dialog box appears.

Step 2 In the flavor list, click on a flavor.

Step 3 In the flavor item list, select a flavor item.

Step 4 For each cell of the flavor item, enter an appropriate new value.

Step 5 For the composite flavors, and for HTTP Content Category flavor:

a) Click in a cell

A Browse button is displayed.

b) Click the **Browse** button.

A Select dialog appears, displaying all valid values for the parameter.

c) Select an appropriate value from the list.

d) Click **OK**.

The Select dialog closes.

The selected value is displayed in the cell.

Step 6 Click **OK**.

The Flavor Settings dialog box closes.

Deleting Flavor Items

To delete a flavor item:

Step 1 From the **Configuration** menu, choose **Flavors**.

The Flavor Settings dialog box appears.

Step 2 In the flavor list, click on a flavor.

Step 3 In the flavor item list, right-click anywhere in a flavor item.

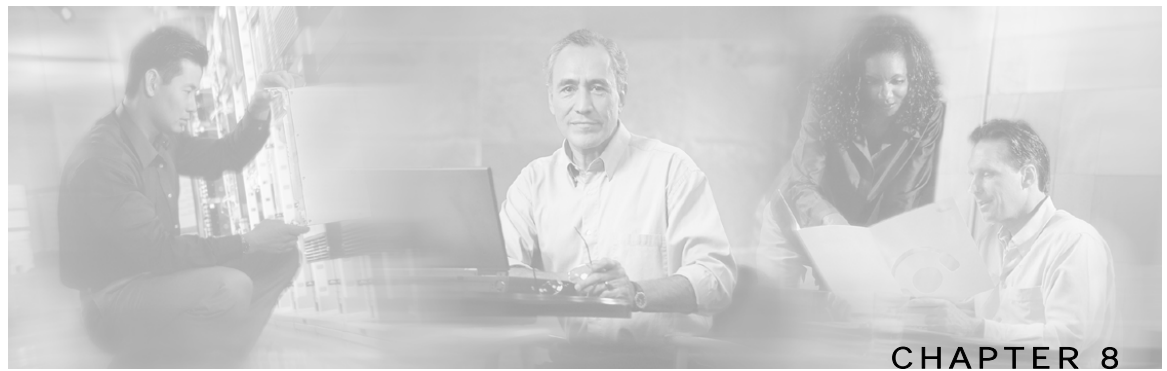
A short-cut menu appears.

Step 4 Click **X 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.



Using the Service Configuration Editor: Traffic Accounting and Reporting

This chapter contains the following sections:

- [Managing Usage Counters 8-1](#)
- [Managing RDR Settings 8-1](#)

Managing Usage Counters

The *Cisco Service Control Application for Broadband (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.

Services may share a usage counter. 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. *Defining Hierarchical Settings for a Service* (on page [7-5](#)) explains how to configure the service hierarchy.

Similarly, packages may share a usage counter; the assignment of packages to usage counters is determined by the package hierarchy. *Setting Advanced Package Options* (on page [9-6](#)) explains how to configure the package hierarchy.

Managing RDR Settings

Service Control Engine (SCE) platforms generate and transmit *Raw Data Records (RDRs)* that contain information that is relevant to the service provider. These RDRs contain a wide variety of information and statistics, depending on the configuration of the system. For more details about the content of each type of RDR, see the *Cisco Service Control Application for Broadband Reference Guide*.



Note

RDRs are not generated for filtered traffic (see *Filtering the Traffic Flows* (on page [10-1](#))).

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—Allows you to enable the generation of each type of Usage RDR, and define their generation intervals
- Traffic Discovery—Allows you to enable the generation of Transaction RDRs and define their maximum rate of generation
- Quota RDRs—Allows you to enable the generation of each type of Quota RDR, and define their generation parameters
- Transaction Usage RDRs—Allows you to specify the packages and services for which Transaction Usage RDRs should be generated
- Log RDRs—Allows you to specify the packages and services for which Log RDRs should be generated
- Real-Time Subscriber RDRs—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—Allows you to specify the packages and services for which Real-Time Signaling RDRs should be generated

Managing Usage RDRs

The SCE platform can generate three types of Usage RDRs. Usage RDRs of each type are generated for each service usage counter; service usage counters aggregate usage for either one service or a group of related services in the services hierarchy.

- Link Usage RDRs—Contain data relating to total usage of a particular group of services for the entire link
- Package Usage RDRs—Contain data relating to total usage of a particular group of services by all subscribers to a particular package
- Subscriber Usage RDRs—Contain data relating to total usage of a particular group of services by a particular subscriber

You can enable or disable the generation of each type of Usage RDR, and set the generation interval for each type of Usage RDR. The generation rate of Subscriber Usage RDRs can be limited (advisable when there are a large number of subscribers).

By default, all three types of Usage RDRs are enabled; each RDR is generated once every five minutes.



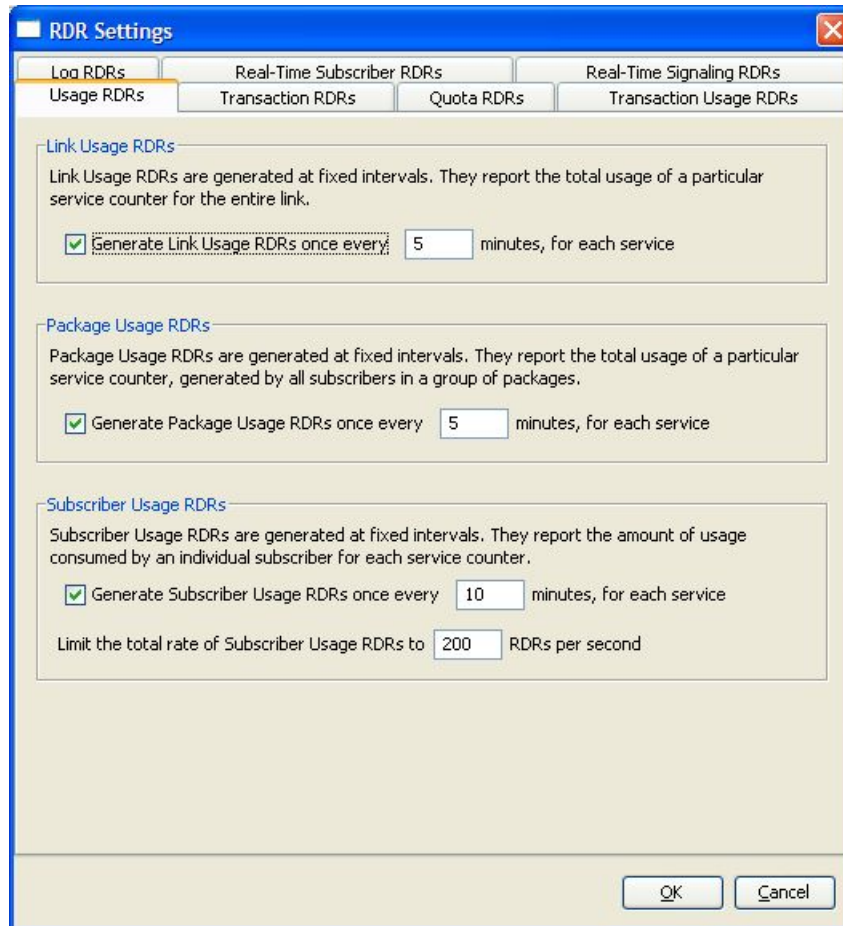
Note

Usage RDRs are not generated for blocked sessions. A session is blocked if the service that the session is mapped to is blocked for this user's package (see *Defining Per-Flow Actions for a Rule* (on page 9-14)), or if the user has exceeded the allowed quota for this service (see *Managing Quotas* (on page 9-48)).

To configure the generation of Usage RDRs:

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

The RDR Settings dialog box appears, open to the **Usage RDR** tab.



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

Managing RDR Settings

Step 5 To configure Transaction RDRs, continue with step 2 of the instructions in the section *Managing Transaction RDRs* (on page 8-4).

Step 6 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of RDRs is saved.

Managing Transaction RDRs

The SCE platform can generate Transaction RDRs for selected service types. Each Transaction RDR contains data about a single network transaction. These RDRs can be used, for example, to generate statistical histograms that help understand the traffic that is traversing the network.

You can enable or disable the generation of Transaction RDRs, set the maximum number of RDRs generated per second, and select for which services the RDRs are generated. You can also assign a relative weight to each service; the relative weight determines the relative number of Transaction RDRs to 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.

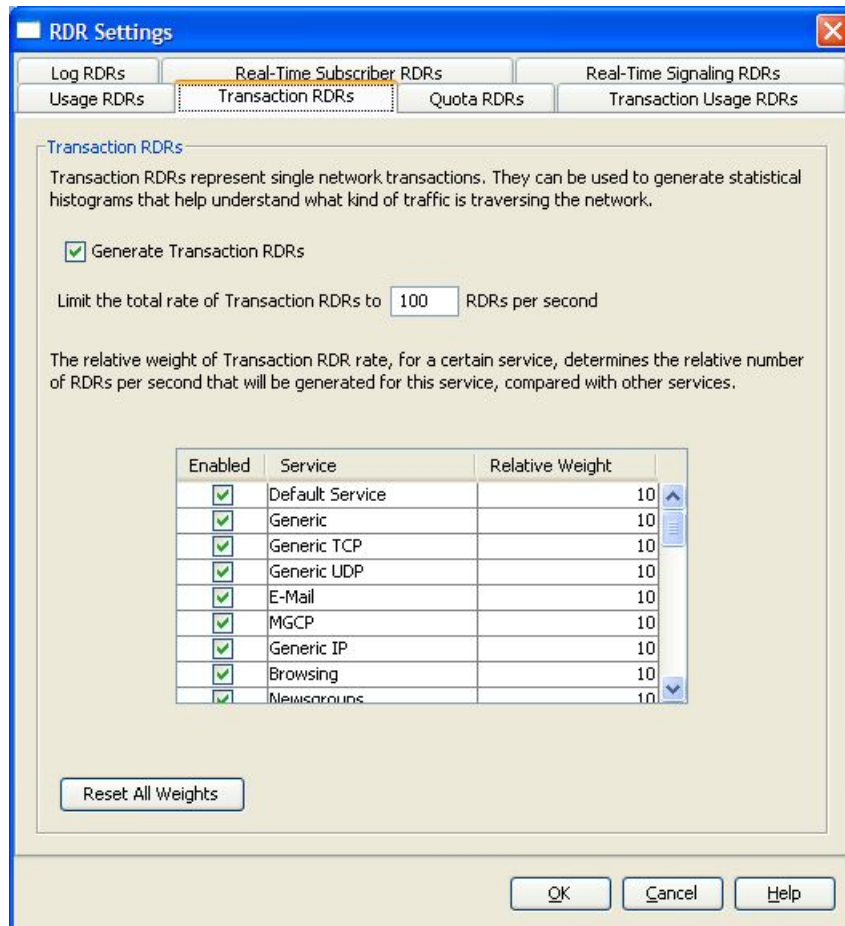
To configure the generation of Transaction RDRs:

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

The RDR Settings dialog box appears.

Step 2 Click the **Traffic Discovery** tab.

The Traffic Discovery tab of the RDR Settings dialog box appears.



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 To configure Quota RDRs, continue with step 2 of the instructions in the section *Managing Quota RDRs* (on page 8-6).

Step 8 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of RDRs is saved.

Managing Quota RDRs

Quota RDRs are generated per subscriber. There are three types of Quota RDRs:

- Quota Breach RDRs—When a quota bucket is depleted, services that try to consume from that bucket are regarded as breached. A Quota Breach RDR can be generated when a quota breach occurs.

When a subscriber's service is breached, it is handled according to the service's breach-handling settings. For example, it is possible to block flows of a specific service once the quota for that service is consumed.

- Remaining Quota RDRs—As quota is consumed, Remaining Quota RDRs can be generated. The Remaining Quota RDR is only generated if a bucket state has change since the last RDR was generated.
- Quota Threshold RDRs—When the remaining quota in a bucket falls below a threshold, a Quota Threshold RDR can be generated. This RDR can be used by external systems; they can treat the RDR as a quota request and provision the subscriber with an additional quota before the bucket is depleted.

Use this tab to enable/disable the generation of Quota RDRs and to define the number of RDRs generated per minute/second.

Each type of Quota RDR can be enabled or disabled. For Remaining Quota RDRs, the generation interval can be set, and the generation rate can be limited (advisable when there are a large number of subscribers). The threshold for Quota Threshold RDRs is also configurable.

By default, all Quota RDRs are disabled.

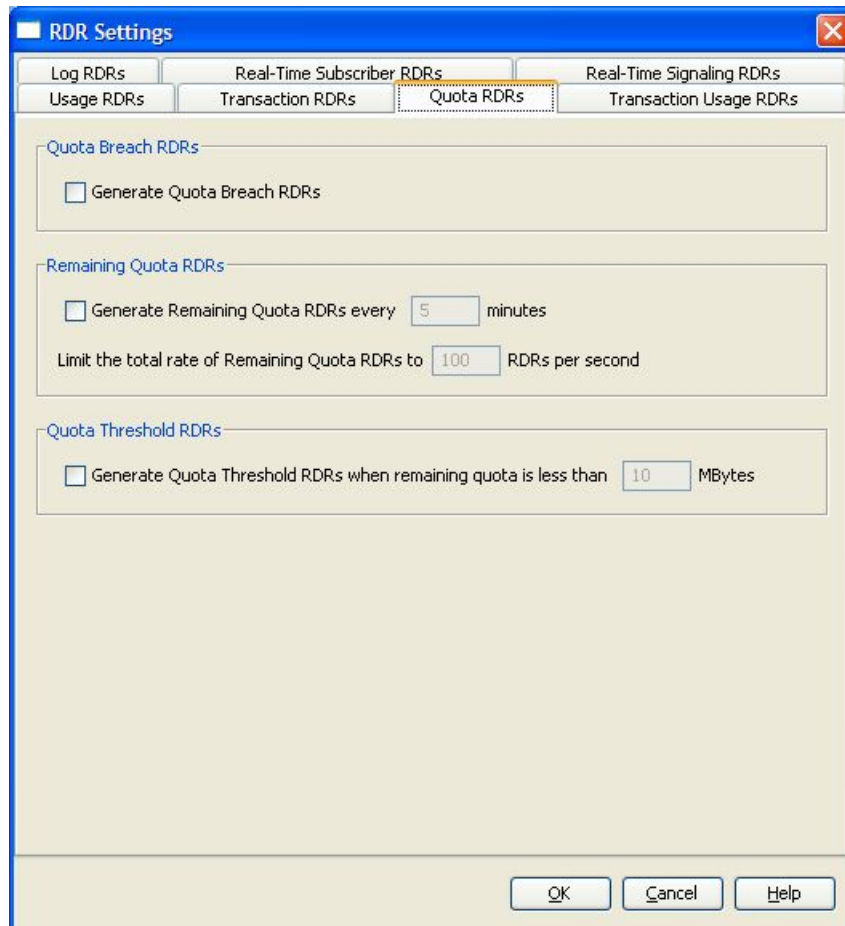
To configure the generation of Quota RDRs:

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

The RDR Settings dialog box appears.

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

The Quota RDRs tab of the RDR Settings dialog box appears.



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:

- Enter the interval in minutes between each generation of the RDR in the Generate Remaining Quota RDRs field

Step 6 To limit the maximum generation rate of Remaining Quota RDRs:

- Enter the maximum number of Remaining Quota RDRs to be generated per second in the Limit the Total Rate of Remaining Quota RDRs field

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:

- Enter the threshold for which Quota Threshold RDR should be generated in the Generate Quota Threshold RDRs field

Managing RDR Settings

Step 9 To configure Transaction Usage RDRs, continue with step 2 of the instructions in the section *Managing Transaction Usage RDRs* (on page 8-8).

Step 10 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of RDRs is saved.

Managing Transaction Usage RDRs

The SCE platform can generate Transaction Usage RDRs for all transactions of selected packages, or for selected services per package. Each Transaction Usage RDR contains data about a single network transaction. These RDRs can be used to build detailed usage logs for specific services and subscribers, suitable, for example, for transaction-based billing.

**Caution**

Generating and collecting an RDR for each transaction can cause performance penalties; enable Transaction Usage RDR generation only for those services and packages that should actually be monitored or controlled by the system.

You can select the packages and services for which Transaction Usage RDRs are generated.

By default, no Transaction Usage RDRs are generated.

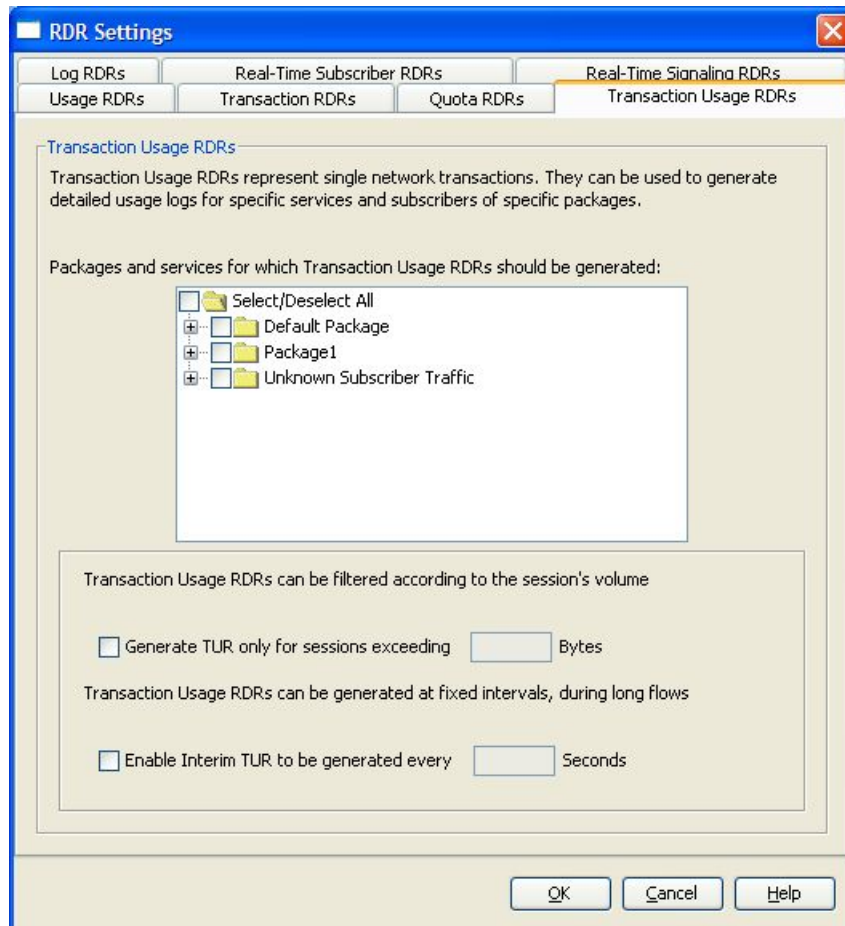
To configure the generation of Transaction Usage RDRs:

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

The RDR Settings dialog box appears.

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

The Transaction Usage RDRs tab of the RDR Settings dialog box appears.



- Step 3** To enable the generation of Transaction Usage 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 4** To 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 desired service.
- Step 5** To limit the generation of Transaction Usage RDRs to 'large' sessions:
- 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** Usually, a Transaction Usage RDR is only generated at when a flow closes. To enable the generation of additional, interim Transaction Usage RDRs for long flows:
- a) Check the **Enable Interim TUR to be generated every** check box.

The Seconds field is enabled.

b) Enter the time in seconds between each generation of a Transaction Usage RDR for each flow.

Step 7 To configure Log RDRs, continue with step 2 of the instructions in the section *Managing Log RDRs* (on page 8-10).

Step 8 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of RDRs is saved.

Managing Log RDRs

Log RDRs provide information regarding system events. They are generated in response to specific actions or state changes. There are two types of Log RDRs:

- Blocking RDRs—Can be generated each time a transaction is blocked
- Breach RDRs—Are generated each time a bucket exceeds the global threshold

You can set the maximum number of Log RDRs generated per second, and select the packages and services for which Blocking RDRs are generated.

By default, Blocking RDRs are generated for all packages; at most 20 Log RDRs are generated per second. Breach RDRs are always generated.

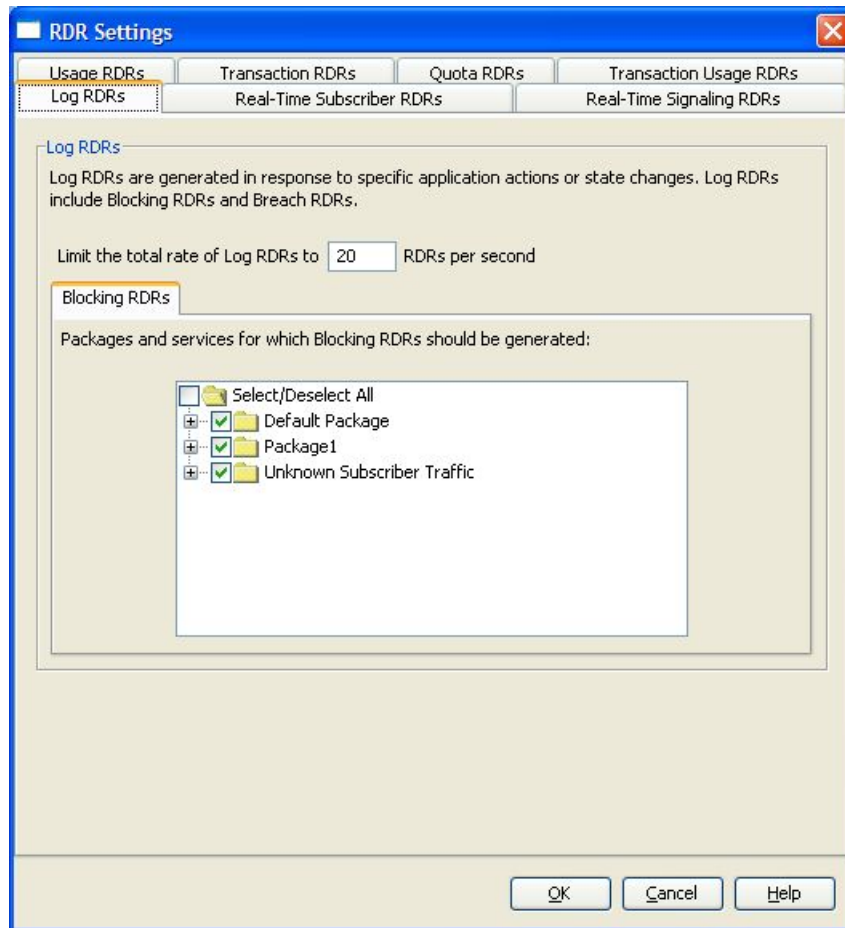
To configure the generation of Log RDRs:

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

The RDR Settings dialog box appears.

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

The Log RDRs tab of the RDR Settings dialog box appears.



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 To enable the generation of Blocking RDRs for selected services of a package:

- Expand the node of the desired package.
- Check the check box next to the service name of each desired service.

Step 6 To configure Real-Time Subscriber RDRs, continue with step 2 of the instructions in the section *Managing Real-Time Subscriber Usage RDRs* (on page 8-12).

Step 7 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of RDRs is saved.

Managing Real-Time Subscriber Usage RDRs

Real-Time Subscriber Usage RDRs are RDRs that report subscriber usage. These RDRs 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.

See *Selecting Subscribers for Real-Time Usage Monitoring* (on page 13-15) for more information on selecting subscribers to be monitored.



Caution

Generating and collecting Real-Time Subscriber Usage RDRs for many subscribers can cause performance penalties; enable Real-Time Subscriber Usage RDR generation only for those subscribers that must actually be monitored by the system.

You can enable or disable the generation of Real-Time Subscriber Usage RDRs, set the generation interval for the RDRs, and set the maximum number of RDRs generated per second.

By default, Real-Time Subscriber Usage RDRs are generated (but only for selected subscribers). An RDR for each subscriber is generated once every minute; at most 100 RDRs are generated per second.

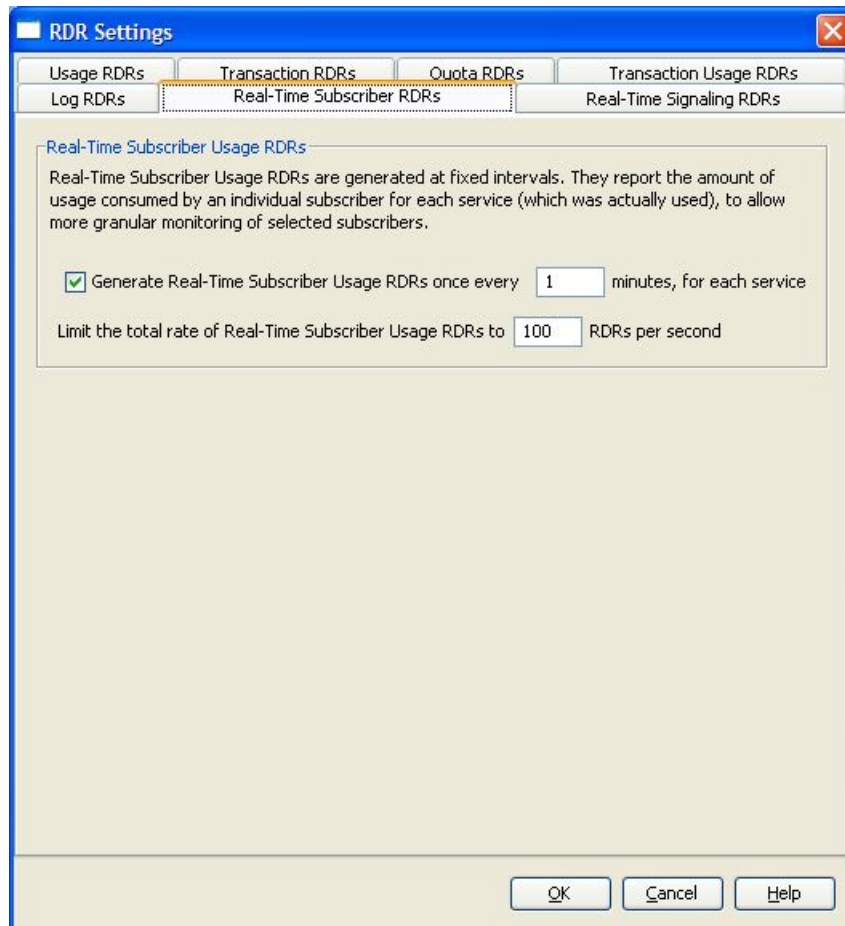
To configure the generation of Real-Time Subscriber Usage RDRs:

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

The RDR Settings dialog box appears.

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

The Real-Time Subscriber RDRs tab of the RDR Settings dialog box appears.



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 To configure Real-Time Signaling RDRs, continue with step 2 of the instructions in the section *Managing Real-Time Signaling RDRs* (on page 8-14).

Step 7 Click **OK**.

The RDR Settings dialog box closes.

The new configuration for the generation of RDRs is saved.

Managing Real-Time Signaling RDRs

Real-Time Signaling RDRs can be 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.

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

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, and set the generation interval for Flow Interim Signaling RDRs. Flow Interim Signaling RDRs can only be generated if Flow Start and Flow Stop Signaling RDRs are enabled.

You can enable or disable the generation of Attack Signaling RDRs for selected packages.

By default, no Real-Time Signaling RDRs are generated

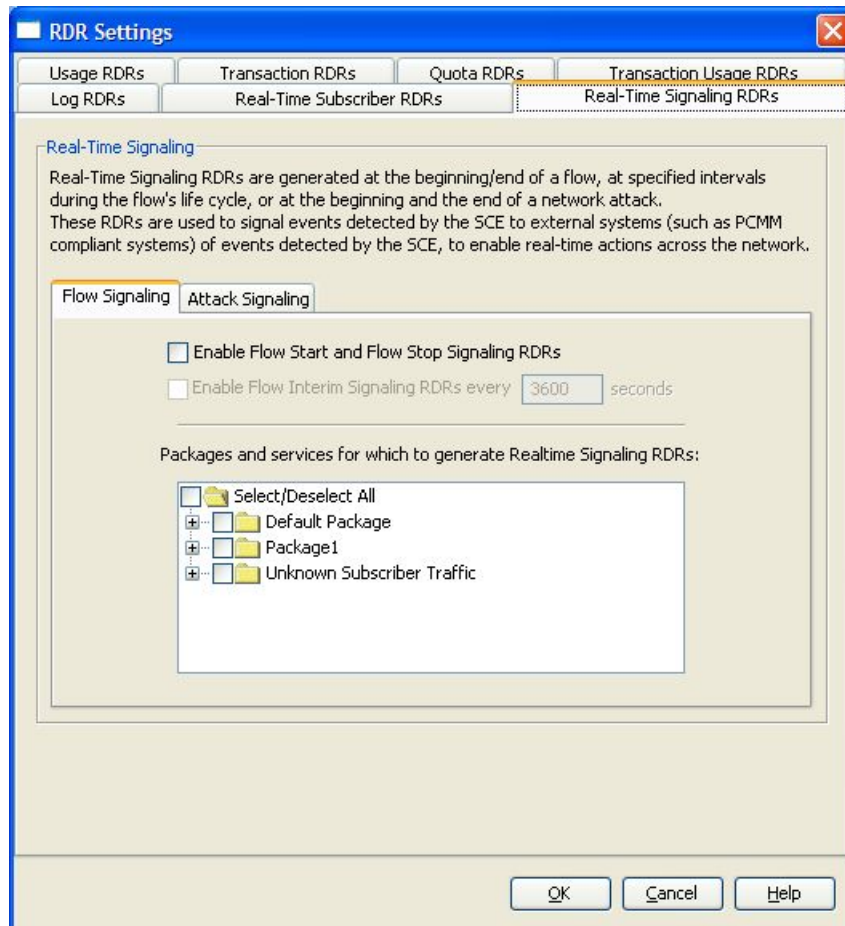
To configure the generation of Real-Time Signaling RDRs:

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

The RDR Settings dialog box appears.

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

The Real-Time Signaling RDRs tab of the RDR Settings dialog box appears.



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
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 seconds 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

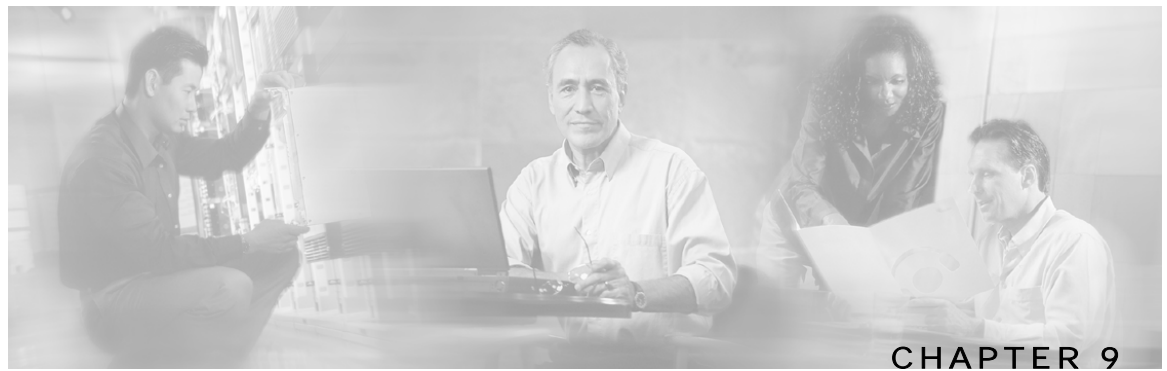
Step 9 To enable the generation of Attack Signaling RDRs for selected packages:

- 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 RDRs is saved.



Using the Service Configuration Editor: Traffic Control

The *Traffic Control* capabilities of the Service Control Engine (SCE) 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-package, and the subscriber's quota state.

This chapter contains the following sections:

- [Managing Packages](#) 9-1
- [Unknown Subscriber Traffic](#) 9-10
- [Managing Rules](#) 9-11
- [Managing Bandwidth](#) 9-31
- [Managing Quotas](#) 9-48

Managing Packages

A *package* is a description of subscriber policy. It determines how each network transaction is controlled.

Packages are collections of rules that define 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* (on page 7-1)) and only then add and define packages.

Every *SCA BB* service configuration contains a *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 non-existent package is assigned to the subscriber.

There can be a maximum of 5000 packages in a service configuration.

Package Parameters

A package is defined by the following parameters:

- General parameters:

- Package Name—Each package must have a unique name.
- Description—An optional description of the package.
- Quota Management parameters:
 - Quota Management Mode—Specifies whether subscriber quotas are managed by an external quota manager or periodically replenished 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 to 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—Each package has a unique package index. The system recognizes packages by their index number; changing the package name does not affect SCE platform activity. A default value of the package index is provided by the system; you should not modify this value.
 - Parent Package—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—Usage counters are used by the system when it generates data about the total use of each package. A package can use an exclusive package usage counter, or use the package usage counter of the parent package.
 - Each usage counter has a name assigned by the system (based on the package name), and a unique counter index. A default value of the counter index is provided by the system; you should not modify this value.
 - Calendar—The calendar that is used as the basis for the time-based rules of the package.
 - VAS Traffic Forwarding Table—The forwarding table used by this package.

These parameters are defined when you add a new package (see *Adding Packages* (on page 9-4)), and can be changed at any time (see *Editing Packages* (on page 9-8)).

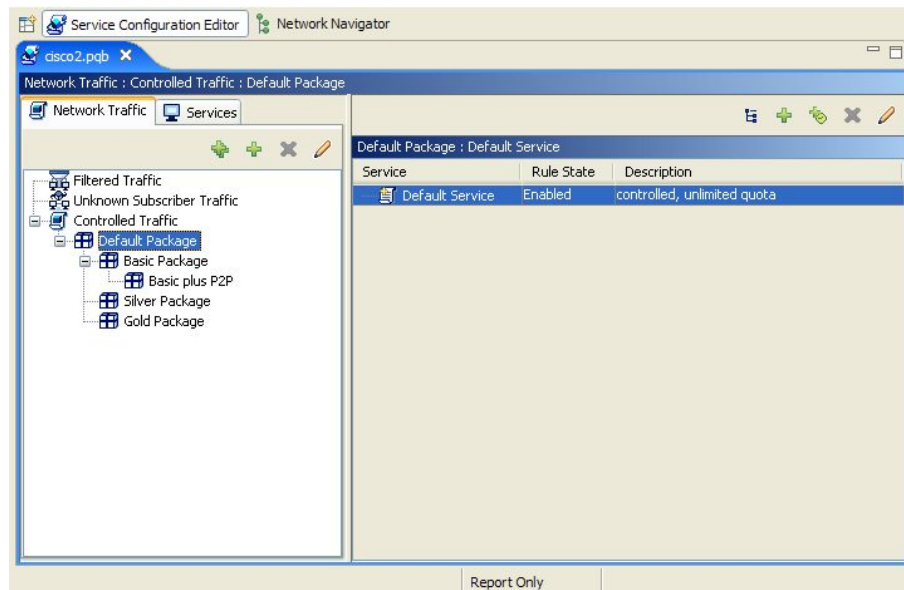
Viewing Packages

You can view a hierarchy tree of all existing packages, and also see a list of services for which specific rules have been defined for any selected package.

To view all packages:

Step 1 In the current service configuration, click the **Network Traffic** tab.

The Network Traffic tab appears.

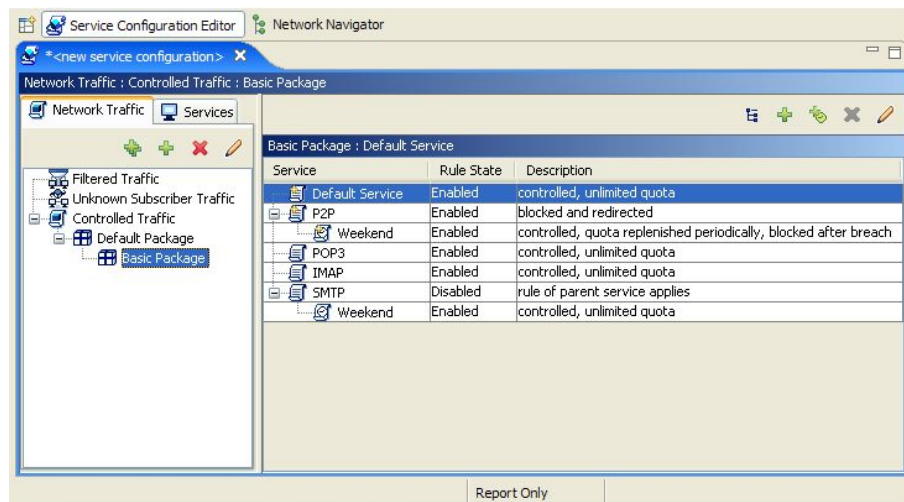


A list of all packages is displayed in the Package hierarchy.

To view more information about a package, open the Package Settings dialog box (*see Editing Packages* (on page 9-8)).

Step 2 Click on a package in the hierarchy to display the rules of the package.

A list of all rules of this package appears in the Rule pane.



Adding Packages

A Default Package is predefined in the SCAS BB Console installation. You can add additional packages to the service configuration.

Adding a package to the Packages hierarchy is the first step in defining a new package.

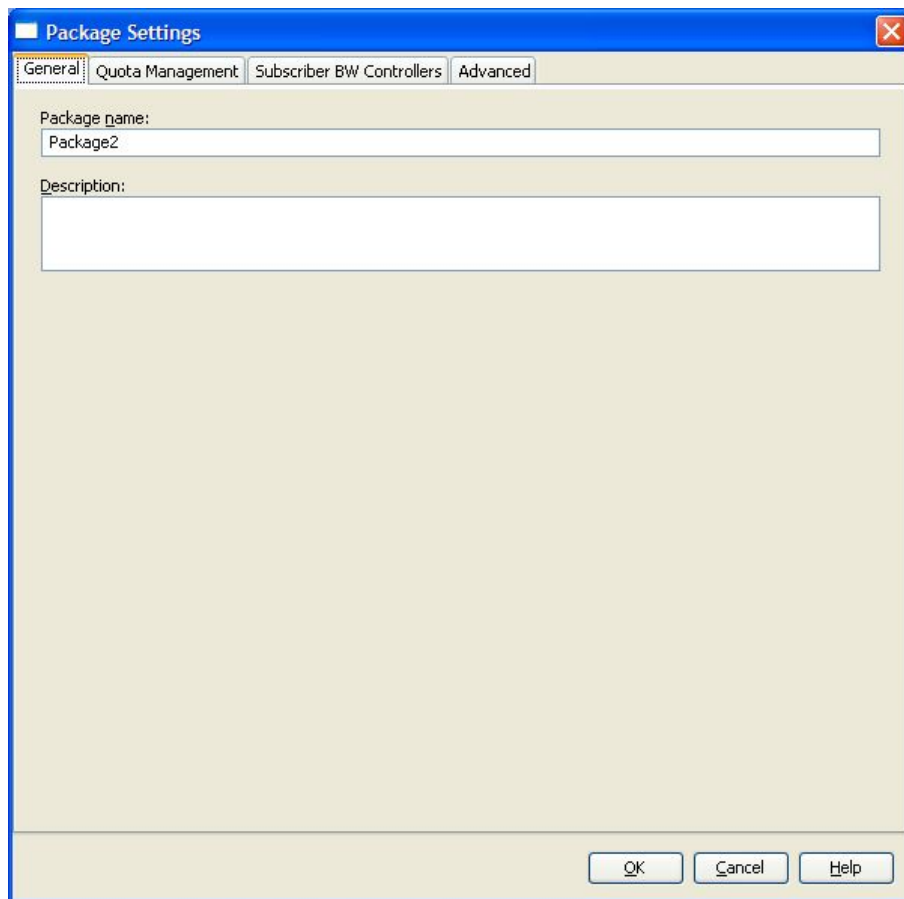
Once you have added and defined a new package, define rules for the package (see *Adding Rules to a Package* (on page 9-12)).

To add a package to the service configuration:

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



This dialog box has the following tabs: General, Quota Management, Subscriber BW Controllers, and Advanced.

Quota management (see *Managing Quotas* (on page 9-48)) and bandwidth management (see *Managing Bandwidth* (on page 9-31)) are aspects of traffic control.

To configure parameters in the Quota Management tab see *Editing Package Quota Management Settings* (on page 9-48), to configure parameters in the Subscriber BW Controllers tab, see *Editing Package Subscriber BWCs* (on page 9-40).

- Step 3** To begin defining the package, continue with the instructions in the section *Defining General Parameters for Packages* (on page 9-5).

Defining General Parameters for Packages

Having added a package to the package hierarchy, you must now set values for its parameters.

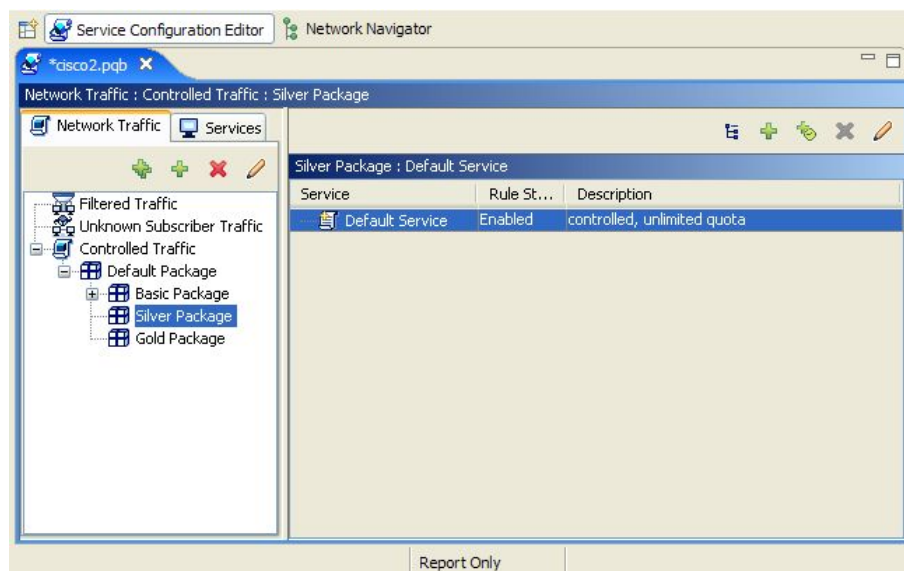
To set the name and description of the package:

When you add a package to the package hierarchy, the Package Settings dialog box appears, open on the General tab.

- Step 1** In the Package name field, enter a unique and relevant name for the package.
- Step 2** (Optional) In the Description field, enter a meaningful and useful description of the package.
- Step 3** To change the index for the package, specify an exclusive usage counter, or select a calendar, continue with the instructions in the section *Setting Advanced Package Options* (on page 9-6).
- Step 4** Click **OK**.

The Package Settings dialog box closes.

The new Package is added as a child to the package selected in the Package hierarchy, and becomes the selected package; the Default Service rule is displayed in the Rule pane.



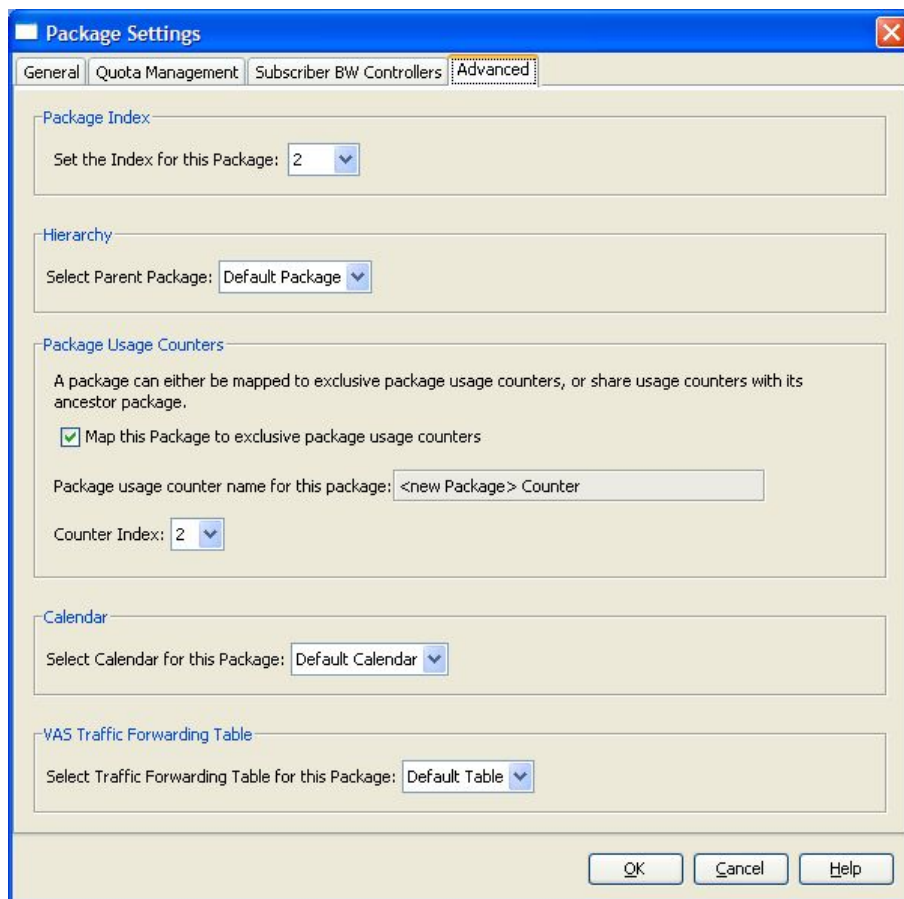
To edit the Default Service rule, and to add new rules to the package, see *Managing Rules* (on page 9-11).

Setting Advanced Package Options

To set the package advanced options:

Step 1 In the Package Settings dialog box, click the **Advanced** tab.

The Advanced tab of the Package Settings dialog box appears.



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

A default value of the counter index is provided by the system; you should 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 the exclusive package usage counter:

- Select a value for the index from the Counter Index drop-down list

A default value of the counter index is provided by the system; you should 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

If VAS traffic forwarding is disabled (the default), the drop-down list is dimmed; to enable VAS traffic forwarding, see *Enabling VAS Traffic Forwarding* (on page 10-24).

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 Rule pane.

To edit the Default Service rule, and to add new rules to the package, see *Managing Rules* (on page 9-11).


Duplicating Packages

You can duplicate an existing package. This is a useful way to add a new package that is 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 hierarchy as the original package.

To duplicate a package:

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

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 more than once).


Step 3 Modify the package parameters as required (see *Editing Packages* (on page 9-8)).

Editing Packages

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

To edit a package:

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

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* (on page 9-48)

Step 6 To change bandwidth control settings:

- See *Editing Package Subscriber BWCs* (on page 9-40)

Step 7 To change advanced settings:

a) Click the **Advanced** tab.

The Advanced tab of the Package Settings dialog box appears.

b) To change the package index for this package:

- From the Set the Index for this Package drop-down list, select a Package Index
-

A default value of the counter index is provided by the system; you should not modify this value unless a specific index value must be assigned to the package.

c) To change the parent package of this package:

- Select the desired parent from the Select Parent Package drop-down list

d) 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

e) 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 enabled

f) 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

A default value of the counter index is provided by the system; you should not modify this value.

g) To change the calendar used by this package:

- Select the desired calendar from the Select Calendar for this Package drop-down list

h) 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

If VAS traffic forwarding is disabled (the default), the drop-down list is dimmed; to enable VAS traffic forwarding, see *Enabling VAS Traffic Forwarding* (on page 10-24).

Step 8 Click **OK**.

The Package Settings dialog box closes.


All changes to the package parameters are saved.

Deleting Packages

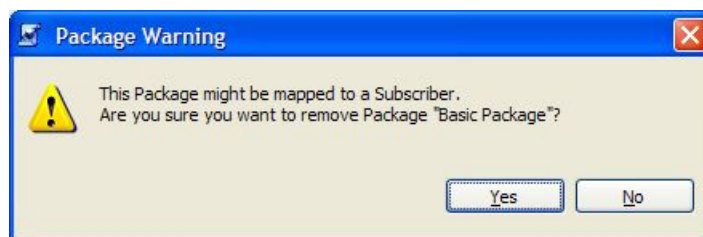
You can delete user-defined packages. The Default Package cannot be deleted.

To delete a package:

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

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

A Package Warning message appears.



Step 3 Click **Yes**.

The package is deleted and is no longer displayed in the Package hierarchy.

Unknown Subscriber Traffic

If a traffic flow does not match any filter rule (see *Filtering the Traffic Flows* (on page 10-1)), and so is processed by the SCE platform, the SCE platform tries to identify the subscriber responsible for the traffic flow. The SCE platform looks at the IP address or VLAN tag of the traffic flow, and checks its internal database for a subscriber that is 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.

The Unknown Subscriber Traffic category appears in the tree in the Network Traffic tab, but it is not part of the package hierarchy. The Unknown Subscriber Traffic category cannot be deleted.

Unknown Subscriber Traffic may be defined as traffic:

- That does not match any Filtered Traffic Rule
- and*
- The IP address or VLAN ID of the flow does not match any subscriber in the database

Traffic of one unknown subscriber cannot be distinguished from traffic of other unknown subscribers. This gives the following limitations when controlling unknown subscriber traffic:

- No per-subscriber usage limits can be defined
- No subscriber-level metering with subscriber BWCs can be defined. Subscriber BWCs can only be used 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
- An exclusive package usage counter is defined; it is named Unknown Subscriber Traffic Counter and has Counter Index = 63

The following procedures are available for the Unknown Subscriber Traffic category:

- Editing the Unknown Subscriber Traffic package settings:
 - Adding extra BWCs (see *Editing Package Subscriber BWCs* (on page 9-40))
 - Selecting a calendar (see *Setting Advanced Package Options* (on page 9-6))
- Editing the Default Service rule:
 - Changing the Rule State (see *Editing Rules* (on page 9-17))
 - Changing per-flow actions for the rule (see *Defining Per-Flow Actions for a Rule* (on page 9-14))
- Adding rules to the Unknown Subscriber Traffic package:
 - Adding rules (see *Adding Rules to a Package* (on page 9-12)); editing (see *Editing Rules* (on page 9-17)) and deleting (see *Deleting Rules* (on page 9-19)) these rules
 - Adding time-based rules (see *Adding Time-Based Rules to a Rule* (on page 9-21)); editing (see *Editing Time-Based Rules* (on page 9-23)) and deleting (see *Deleting Time-Based Rules* (on page 9-25)) these rules

Managing Rules

Once services and basic packages have been defined, you can define *rules* for the package.

Rules can be configured to do some or all of the following:

- Block the service
- Set a quota for the service
- Define maximum bandwidth for the service
- Define behavior when the quota for this service is breached

A rule usually applies at all times. To allow additional flexibility, the week can be divided into four separate *time frames*, and sub-rules - *time-based rules* - can be defined for each time frame.

Viewing 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 the rule applies to, whether the rule is enabled or disabled, and a brief description of the rule.

To see more information about a rule, open the Edit Rule for Service dialog box (see *Editing Rules* (on page 9-17)).

To see more information about a time-based rule, open the Edit Time-Based Rule for Service dialog box (see *Editing Time-Based Rules* (on page 9-23)).

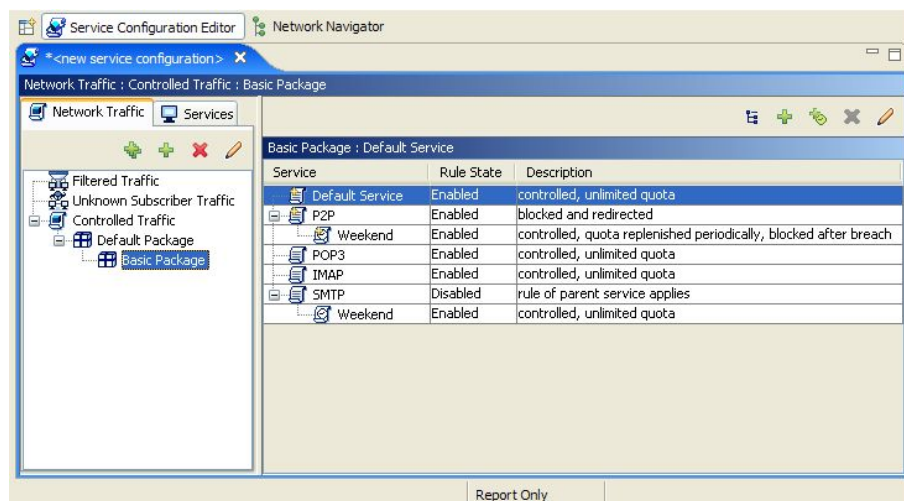
To view the rules of a package:

Step 1 In the current service configuration, click the **Network Traffic** tab.

The Network Traffic tab appears.

Step 2 In the Network Traffic tab, select a package from the package tree.

A list of all rules defined for this package appears in the Rule pane.



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 BW Controllers (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 that is mapped to the POP3 service will be handled according to the POP3 rule; any flow that is mapped to the SMTP or IMAP service will be handled according to the E-Mail rule. This means, for instance, that POP3 can have its own usage limits, while SMTP and IMAP must share usage limits.



Note

If you add a rule for a child service, the settings for the ancestor 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 an icon including a plus sign (). 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 .

Also see *Displaying the Services Affected by a Rule* (on page [9-20](#)).

Adding Rules to a Package

A Default Service rule is assigned to every package. You can add additional rules to a package.

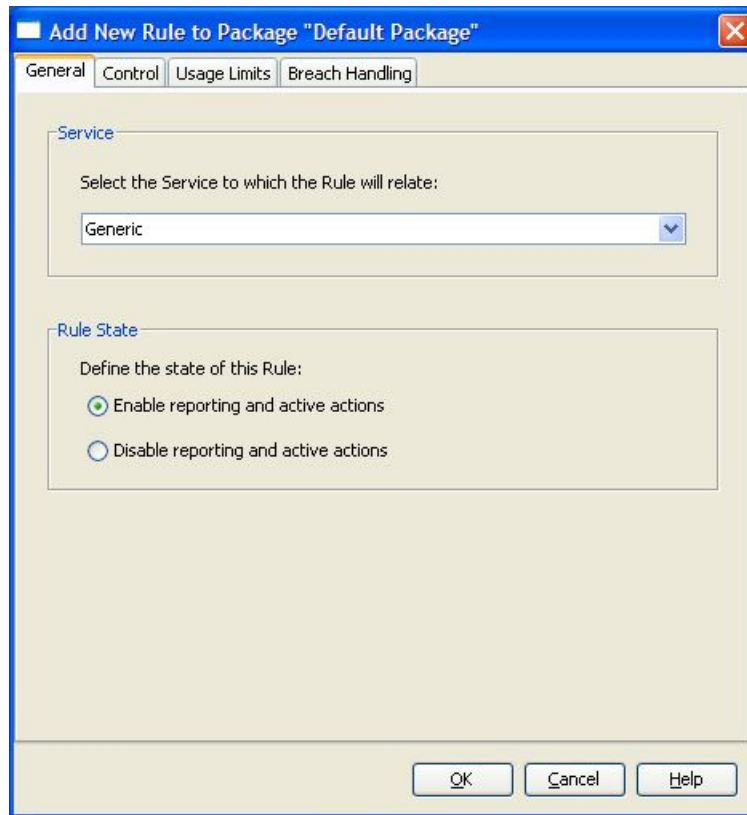
Adding time-based rules is described in the section *Adding Time-Based Rules to a Rule* (on page [9-21](#)).

To add a rule to a package:

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

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

The Add New Rule to Package dialog box appears.



This dialog box has the following tabs: General, Control, Usage Limits, and Breach Handling.

Usage limits and breach handling are part of quota management (see *Managing Quotas* (on page 9-48)): to configure parameters in the Usage Limits tab see *Selecting Quota Buckets for Rules* (on page 9-49), to configure parameters in the Breach Handling tab, see *Editing Breach Handling Parameters for a Rule* (on page 9-51).

Step 3 To begin defining the rule, continue with the instructions in the section *Defining General Parameters for a Rule* (on page 9-13).

Defining General Parameters for a Rule

The General tab of the Add New Rule to Package dialog box has two areas:

- Service—Used to select the service to which this rule will be applied
- Rule State—Used to select the state of the rule

To set the service and state of the rule:

Step 1 In the Service area, select a service from the Select the Service to Which the Rule will Relate drop-down list.

Services for which a rule is already defined are dimmed.

Step 2 In the Rule State area, click one of the **Define the State of this Rule** radio buttons:

- **Enable reporting and active actions**
- **Disable reporting and active actions**

You can enable or disable a rule at any time (see *Editing Rules* (on page 9-17)).

Step 3 To set behavior per traffic-flow for this rule, continue with the instructions in the *section Defining Per-Flow Actions for a Rule* (on page 9-14).

Step 4 Click **OK**.

The Add New Rule to Package dialog box closes.

The new rule is added to the list of rules displayed in the Rule pane.

Defining 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.

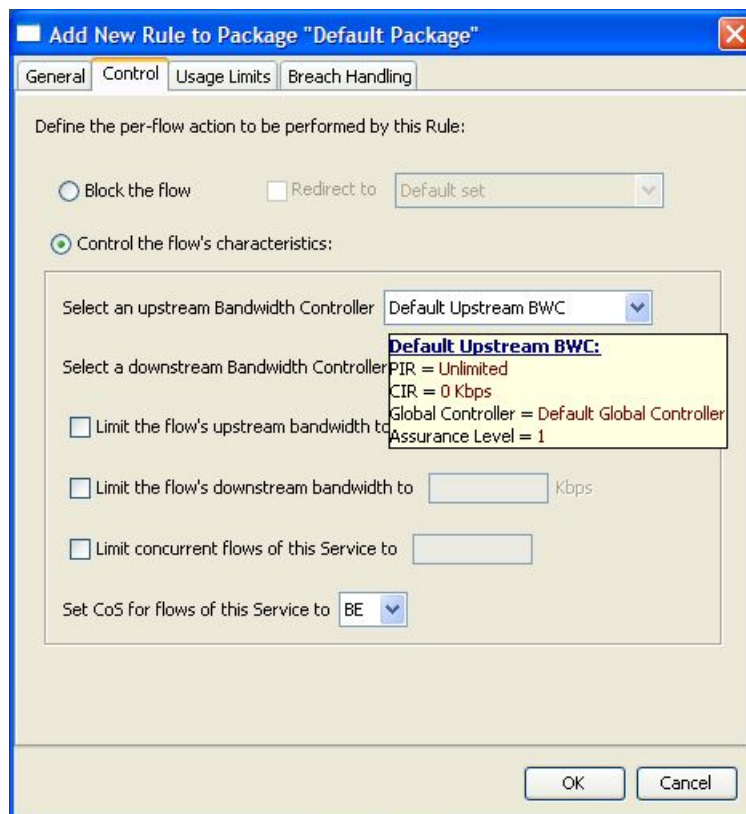
When you select the **Control** tab, the following dialog box appears.

The screenshot shows the 'Add New Rule to Package' dialog box with the 'Control' tab selected. The dialog box has a title bar with a close button (X) and a tab bar with 'General', 'Control', 'Usage Limits', and 'Breach Handling'. The 'Control' tab is active, and the text 'Define the per-flow action to be performed by this Rule:' is displayed. There are two radio buttons: 'Block the flow' (unselected) and 'Control the flow's characteristics:' (selected). The 'Block the flow' option has a 'Redirect to' dropdown menu set to 'Default set'. The 'Control the flow's characteristics:' option has a sub-dialog box with the following controls: 'Select an upstream Bandwidth Controller' (dropdown set to 'Default Upstream BWC'), 'Select a downstream Bandwidth Controller' (dropdown set to 'Default Downstream BWC'), three checkboxes for bandwidth limits (all unselected) with input fields and 'Kbps' labels, and 'Set CoS for flows of this Service to' (dropdown set to 'BE'). At the bottom of the dialog box are 'OK', 'Cancel', and 'Help' buttons.

The dialog box has two main sections. In the upper section you determine what happens to flows identified as belonging to this rule:

- **Block the flow**—When you select this radio button, the Redirect option is enabled:
 - **Redirect to**—If you check the **Redirect to** check box, the Redirection URL Set drop-down list is enabled. From this drop-down list, select the URL set that is to serve as the redirection target. URL redirection sets are defined in the System Settings dialog box. (See *Configuring the Redirection Parameters* (on page 10-19).) Only three protocol types support redirection: HTTP, HTTP Streaming, and RTSP.
- **Control the flow characteristics**—When you select this radio button the options in the second half of the dialog box are enabled:
 - **Select an upstream Bandwidth Controller**—The BWCs in this drop-down list are defined when creating or editing the package (see *Editing Package Subscriber BWCs* (on page 9-40)). Use this option to map this rule's traffic flows to a specific upstream BWC. This sets up bandwidth metering of all concurrent flows mapped to this rule, based on the characteristics of the selected BWC.

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



- **Select a downstream Bandwidth Controller**—The same functionality as the previous option, but for the downstream side of the flow.
- **Limit the flow's upstream bandwidth**—Used to set a per-flow upstream bandwidth limit (for flows mapped to the service of this rule).

- **Limit the flow's downstream bandwidth**—Used to set a per-flow downstream bandwidth limit.
- **Limit concurrent flows of this Service**—Use this option to set the maximum number of concurrent flows (mapped to this rule) permitted to a subscriber.
- **Set CoS for flows of this Service**—Used to set the class-of-service for flows mapped to the service of this rule. Default is BE (best effort).

To define the traffic-flow behavior of the rule:

Step 1 Click the **Control** tab.

The Control tab of the Add New Rule to Package dialog box appears.

Step 2 To control and define the flow's characteristics, continue at step 4.

To block flow's that are mapped to the service of this rule:

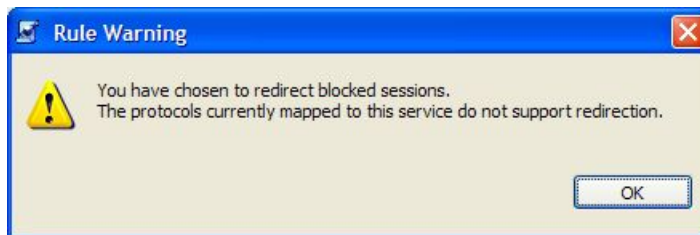
- a) Click the **Block the flow** radio button

The Redirect check box is enabled.

- b) (Optional) To redirect blocked flows (for HTTP, HTTP Streaming, and RTSP), check the **Redirect to** check box.

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** to continue.

- c) Select a redirection URL set from the Redirect drop-down list.

Step 3 Continue at step 5.

Step 4 Click 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
- 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 **Limit concurrent flows of this Service** check box and enter a value in the associated field
- From the Set CoS for flows of this Service drop-down list, select a class-of-service

Step 5 Click **OK**.

The Add New Rule to Package dialog box closes.

The new rule is added to the list of rules displayed in the Rule pane.

Editing Rules

You can edit any rule, including the Default Service rule.



Note You cannot disable the Default Service rule.

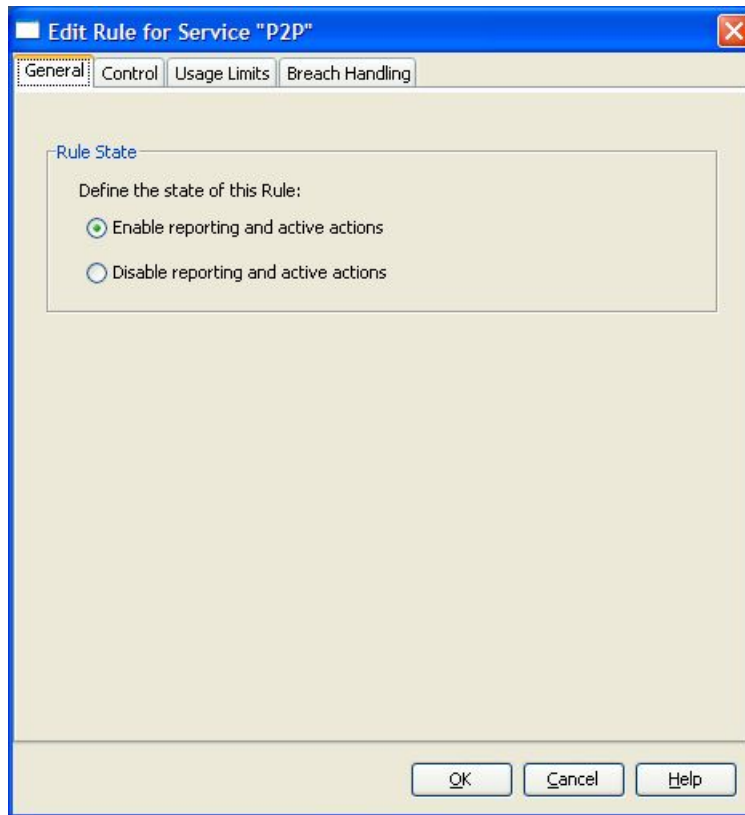
To edit a rule:

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

Step 2 In the 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, click one of the **Define the State of this Rule** radio buttons:

- **Enable reporting and active actions**
- **Disable reporting and active actions**

Step 5 To change behavior per traffic-flow:

a) Click the **Control** tab.

The Control tab of the Edit Rule for Service dialog box appears.

b) Follow the instructions in *Defining Per-Flow Actions for a Rule* (on page 9-14).

Step 6 To change usage limits:

a) Click the **Usage Limits** tab.

The Usage Limits tab of the Edit Rule for Service dialog box appears.

b) Follow the instructions in *Selecting Quota Buckets for Rules* (on page 9-49).

Step 7 To define behavior when a quota is breached:

a) Click the **Breach Handling** tab.

The Breach Handling tab of the Edit Rule for Service dialog box appears.

b) Follow the instructions in *Editing Breach Handling Parameters for a Rule* (on page 9-51).

Step 8 Click **OK**.

The Edit Rule for Service dialog box closes.

All changes to the rule are saved.

**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.

Deleting 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 *Editing Rules* (on 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.

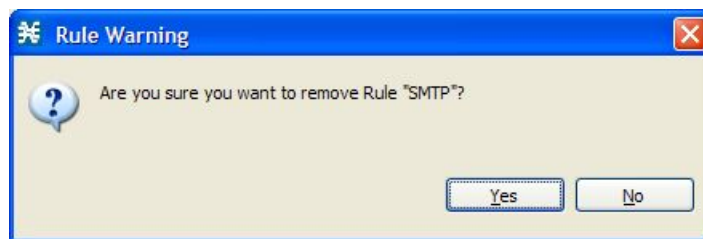
To delete a rule:

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

Step 2 In the Rule pane, select a rule.

Step 3 In the Rule pane, click  (**Remove Rule**).

A Rule Warning message appears.



Step 4 Click **Yes**.

The selected rule is deleted.

Displaying the Services Affected by a Rule

Services can be defined as the children 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 the service's children is indicated in the rules list by a small yellow plus-sign ('+') on the icon, as illustrated for the Default Service rule and P2P rule in the following figure.

Service	Rule State	Description
Default Service	Enabled	controlled, unlimited quota
+ P2P	Enabled	blocked and redirected
POP3	Enabled	controlled, unlimited quota
IMAP	Enabled	controlled, unlimited quota
SMTP	Disabled	rule of parent service applies

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

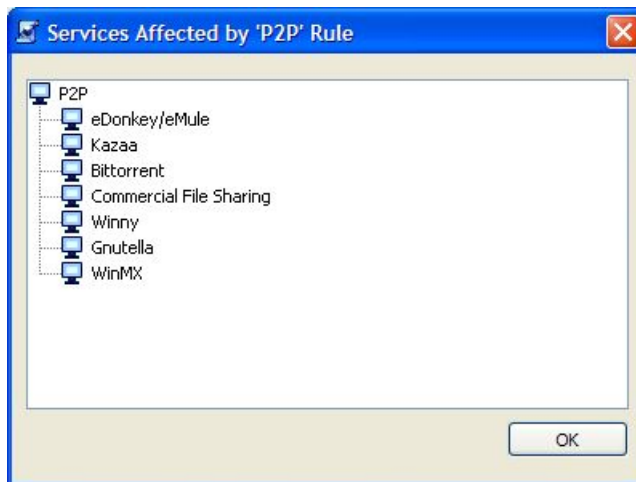


Note The Default Service rule always affects all other services until rules are defined for those services.

To display all services that are affected by a specific rule:

Step 1 Select the rule in the rules list and click  (**Show All Services Affected By This Rule**).

The Service Affected dialog box appears.



Step 2 Click **OK**.

The Service Affected dialog box closes.

Managing Time-Based Rules

The SCAS BB Console allows you to split the week into four *time frames* (see *Managing Calendars* (on page 9-26)). 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, the rules for the different time frames will 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 then 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.

Adding Time-Based Rules to a Rule


You can add a time-based rule to any rule. Adding a time-based 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 original rule is enforced.



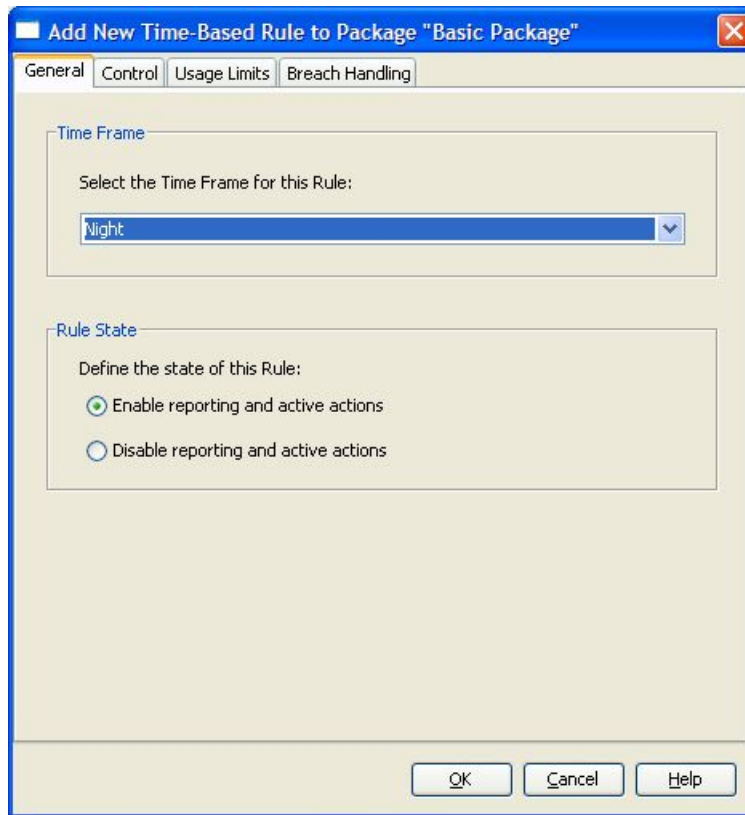
Note

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.

To add a time-based rule:

- Step 1** In the Network Traffic tab, select a package from the package tree.
- Step 2** In the 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, click one of the **Define the State of this Rule** radio buttons:
- **Enable reporting and active actions**
 - **Disable reporting and active actions**
- Step 6** To define behavior per traffic-flow:
- a) Click the **Control** tab.
The Control tab of the Add New Time-Based Rule dialog box appears.
 - b) Follow the instructions in *Defining Per-Flow Actions for a Rule* (on page 9-14).
- Step 7** To change usage limits:
- a) Click the **Usage Limits** tab.
The Usage Limits tab of the Add New Time-Based Rule dialog box appears.
 - b) Follow the instructions in *Selecting Quota Buckets for Rules* (on page 9-49).
- Step 8** To define behavior when a quota is breached:
- a) Click the **Breach Handling** tab.
The Breach Handling tab of the Add New Time-Based Rule dialog box appears.

b) Follow the instructions in *Editing Breach Handling Parameters for a Rule* (on page 9-51).

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.



Note

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 small yellow plus-sign ('+') on the icon of the rule, as illustrated for the Weekend time-based rule of the P2P rule in the following graphic.

Service	Rule State	Description
Default Service	Enabled	controlled, unlimited quota
P2P	Enabled	blocked and redirected
Weekend	Enabled	controlled, quota replenished periodically, blocked after breach
POP3	Enabled	controlled, unlimited quota
IMAP	Enabled	controlled, unlimited quota
SMTP	Disabled	rule of parent service applies
Weekend	Enabled	controlled, unlimited quota

Editing Time-Based Rules

You can edit time-based rules.

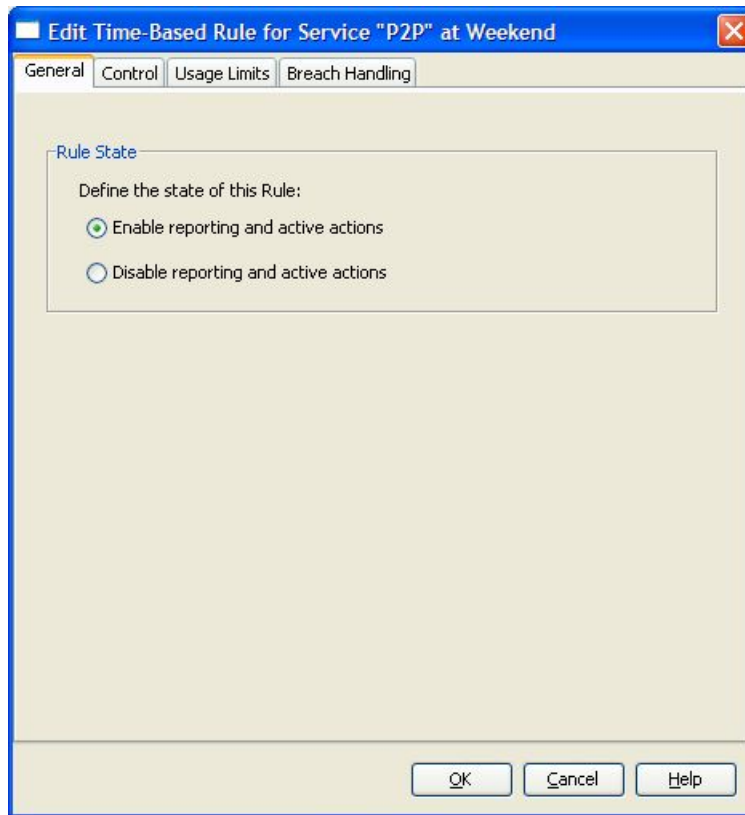
To edit a time-based rule:

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

Step 2 In the 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, click one of the **Define the State of this Rule** radio buttons:

- **Enable reporting and active actions**
- **Disable reporting and active actions**

Step 5 To change behavior per traffic-flow:

a) Click the **Control** tab.

The Control tab of the Edit Time-Based Rule for Service dialog box appears.

b) Follow the instructions in *Defining Per-Flow Actions for a Rule* (on page 9-14).

Step 6 To change usage limits:

a) Click the **Usage Limits** tab.

The Usage Limits tab of the Edit Time-Based Rule for Service dialog box appears.

b) Follow the instructions in *Selecting Quota Buckets for Rules* (on page 9-49).

Step 7 To define behavior when a quota is breached:

a) Click the **Breach Handling** tab.

The Breach Handling tab of the Edit Time-Based Rule for Service dialog box appears.

b) Follow the instructions in *Editing Breach Handling Parameters for a Rule* (on page 9-51).

Step 8 Click **OK**.

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

All changes to the time-based rule are saved.



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.

Deleting Time-Based Rules

You can delete any time-based rule.




Note You can *disable* a rule without losing its profile (see *Editing Time-Based Rules* (on page 9-23)). This allows you to enable the rule again later, without having to reset all its parameters.

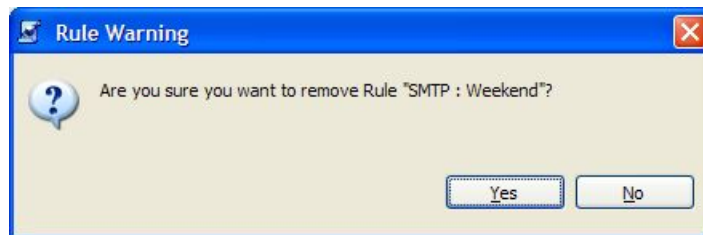
To delete a time-based rule:

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

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

Step 3 In the Rule pane, click  (**Remove Rule**).

A Rule Warning message appears.



Step 4 Click **Yes**.

The selected rule is deleted.

Managing Calendars

Calendars are used to split the hours of the week into four *time frames*.

Once you have configured a calendar, you can add time-cased rules to a package that is using 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 only apply 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. In addition, you can add another nine calendars, each with a different time-frame configuration. Different calendars can be used for different packages. They can also be used where a service provider has customers in more than one time zone; calendars can be configured with a one hour offset from each other.

Managing calendars includes the following:

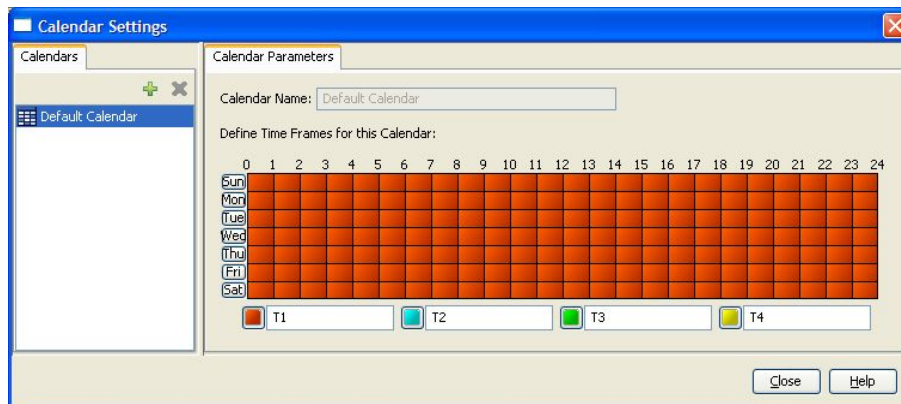
- **Viewing Calendars** (on page 9-26)—Display a list of existing calendars and their time frames
- **Adding Calendars** (on page 9-27)—Add additional calendars
- **Renaming the Time Frames** (on page 9-28)—Set names for the time frames
- **Deleting Calendars** (on page 9-29)—Delete any user-added calendar
- **Configuring the Time Frames** (on page 9-29)—Assign the hours of the week to the time frames

Viewing Calendars

To view the weekly calendars:

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

The Calendars Settings dialog box appears.



The Calendars tab displays a list of existing calendars. Click on 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 Calendars Settings dialog box closes.

Adding Calendars

Each service configuration includes one Default Calendar; you can add up to nine more calendars.

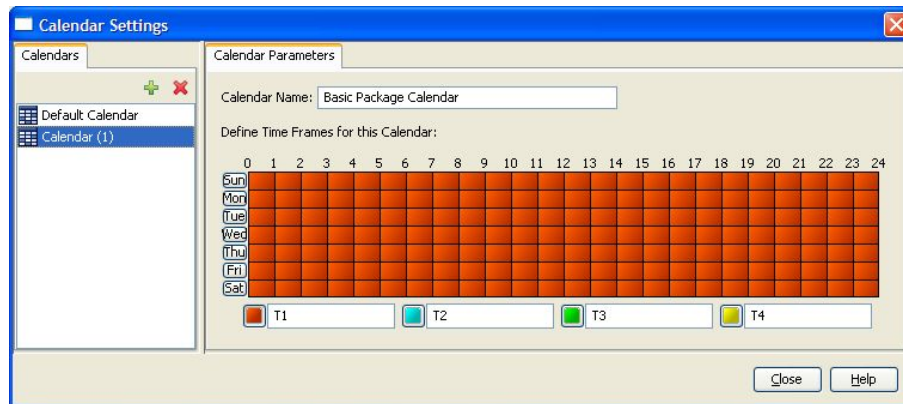
To add a calendar:

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

The Calendars 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 Calendars Settings dialog box closes, and the new calendar name is saved.

If you click **X** to close the dialog box, the name change is not saved.

Renaming 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 the time frames can be configured 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.

To rename the time frames:

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

The Calendars 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 Calendars Settings dialog box closes, and the changes to the names of the time frames are saved.

If you click **X** to close the dialog box, the name changes are not saved.

Deleting Calendars

You can delete any user-added calendar. The Default Calendar cannot be deleted.




Note A calendar that is being used by any package cannot be deleted. (When you select the calendar, the Remove icon is dimmed.) To delete the calendar, you must first select a different calendar for each package that is using the calendar that is to be deleted. See *Setting Advanced Package Options* (on page 9-6) for information about changing the calendar that is associated with a package.

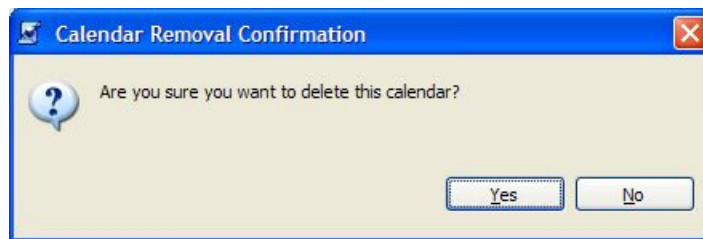
To delete a calendar:

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

The Calendars Settings dialog box appears.

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

A Calendar Removal Confirmation message appears.



Step 3 Click **Yes**.

The calendar is deleted.

Step 4 Click **Close**.

The Calendars Settings dialog box closes.

Configuring the Time Frames

The SCAS BB Console allows you to divide the week into four separate time frames. These time frames allow time-dependent differentiated services to be supplied and can be used to impose constraints on any service.

You might want, for example, to divide the week as follows:

- Peak
- Off Peak
- Night

- Weekend

A week is divided into time frames by assigning each of the 168 (24x7) hours of the week to one of the four time frames. By default, all the hours of the week belong to one time frame.

You can define different time frames for each calendar.

To configure the time frames:

Step 1 From the **Configuration** menu, choose **Weekly Time Frames**.

The Calendars Settings dialog box appears.

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

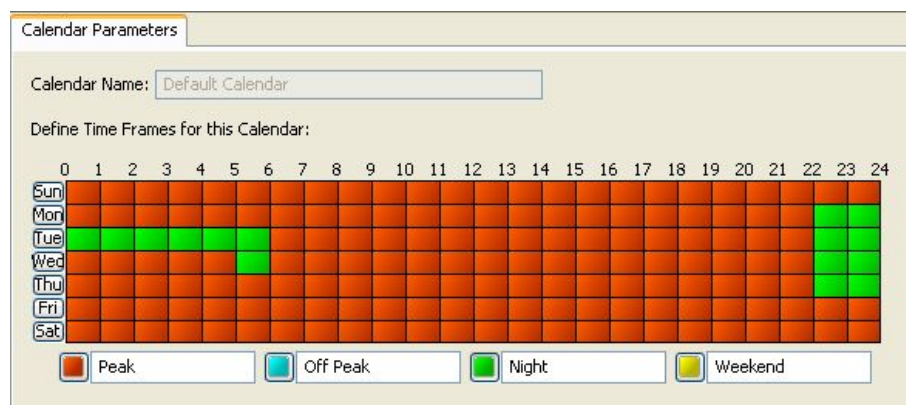
In the Calendar Parameters tab, a grid labeled **Define Time Frames for this Calendar** appears. The grid represents one week, and is laid out in a format of 24 hours x 7 days, where each cell represents one hour.

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 should be part of the selected time frame.

To select a group of cells, hold down the mouse button, and drag across the cells.



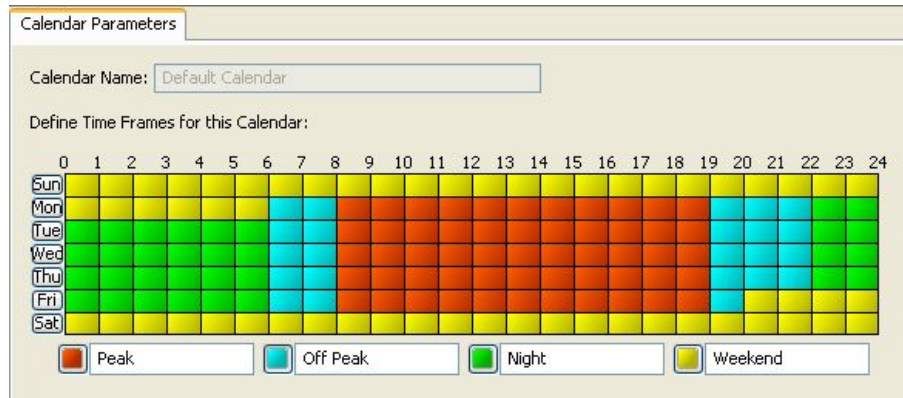
The changes are written to the service configuration as you make them.

Step 5 Repeat steps 3 and 4 for the other time frames until you have mapped the entire grid. You can change the grid by overwriting with another color.

Step 6 Click **Close** when you have completed the time-frame mapping.

The Calendars Settings dialog box closes.

You have now mapped the week into four different time frames. The following figure illustrates a possible time partition plan:



Managing Bandwidth

The upstream and downstream interfaces are each assigned one Default Global Controller. You can add additional global controllers.

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

Managing Global Bandwidth

The upstream and downstream interfaces are each assigned one Default Global Controller that, by default, controls 100% of the link traffic. You can add up to 63 more global controllers for each interface, and assign a maximum percentage of the total link limit to each global controller separately.

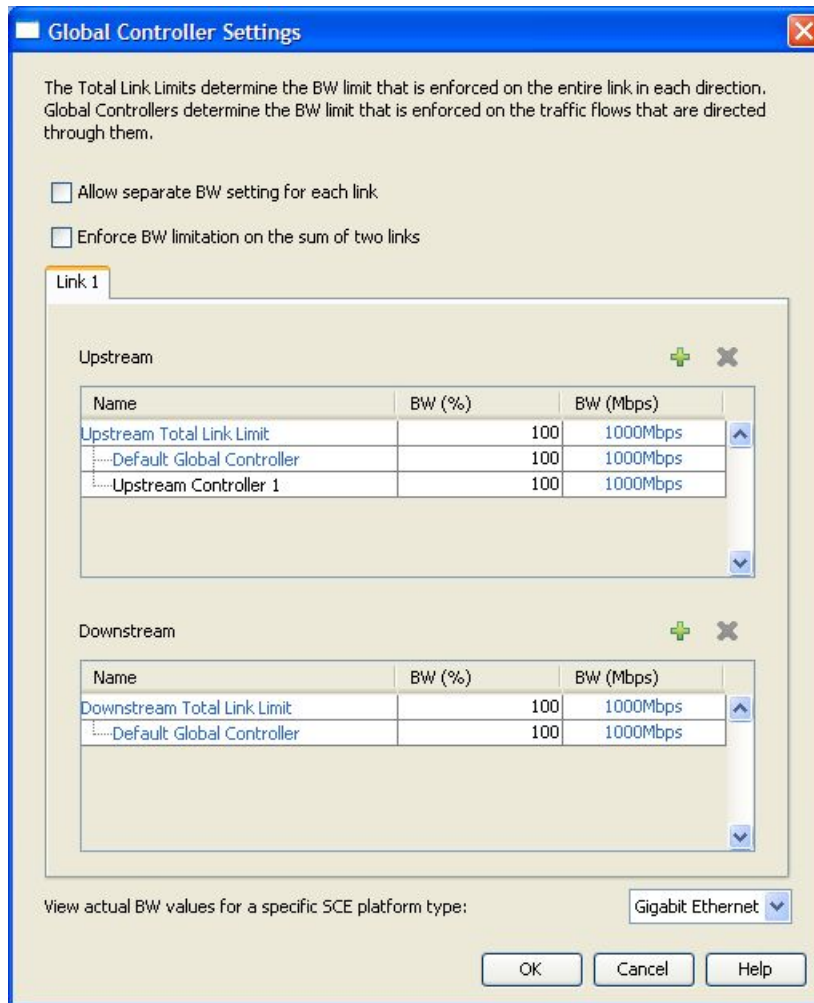
You can also define the bandwidth total link limit to be less than the physical capacity of the SCE platform for each interface separately. When another device sitting next to the SCE platform on the IP stream has limited BW capacity, you can enforce this limitation in a policy-aware manner (by the SCE platform), instead of it being arbitrarily enforced by the other device.

Viewing Global Controller Settings

To view global controller settings:

-
- Step 1** From the **Configuration** menu, choose **Global Controllers**.

The Global Controller Settings dialog box appears.



At the top of the Global Controller Settings dialog box are two check boxes. These are only used in dual link systems (see *Defining Global Controllers in a Dual Link System* (on page 9-36)).

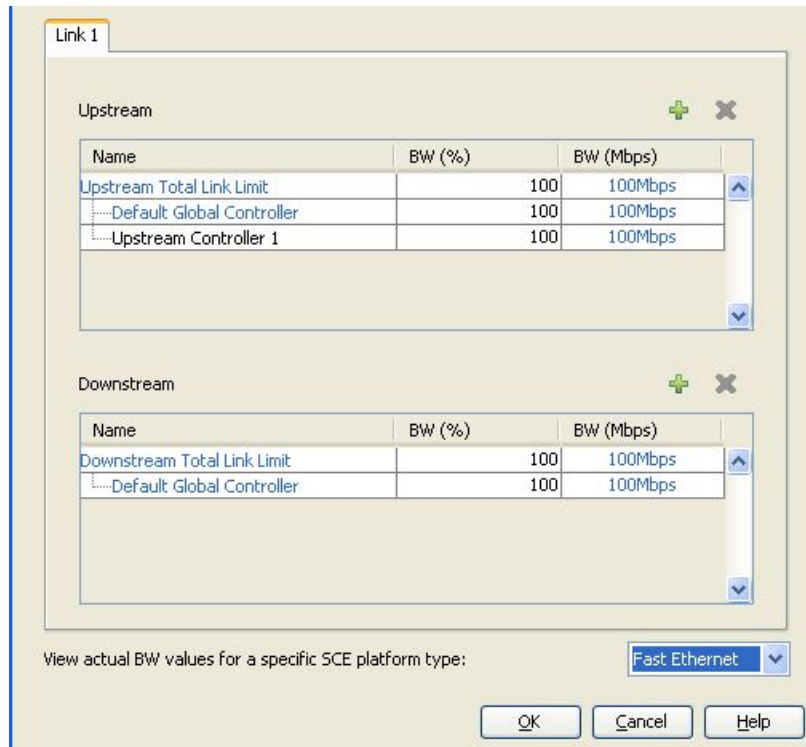
In the center of the dialog box is the Link 1 tab. This has one area listing upstream global controllers and a second area listing downstream global controllers. Each list has three columns:

- **Name**—*Display only*. A unique name assigned to the global controller. The system automatically assigns the names Controller 1, Controller 2, and so on.
- **BW (%)**—The maximum percentage of the total link limit permitted to this global controller.
- **BW (Mbps)**—The actual maximum bandwidth permitted to this global controller, in Mbps. This figure is calculated automatically by the system based on the SCE platform type (Gigabit Ethernet or Fast Ethernet), the controller maximum bandwidth percentage and the total link bandwidth percentage.

Step 2 To view the actual bandwidth values in the BW (Mbps) column, select the desired platform type from the View actual BW values for a specific SCE platform type drop-down list in the lower right-hand corner of the dialog box.



The BW (Mbps) column values change to reflect the choice.



Step 3 Click **OK**.

The Global Controller Settings dialog box closes.

Editing 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.

To edit the total link limit:

Step 1 From the **Configuration** menu, choose **Global Controllers**.

The Global Controller Settings dialog box appears.

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

The values in all the BW (Mbps) cells change to reflect the new total link limit.

Step 3 Click **OK**.

Your changes are saved.

The Global Controller Settings dialog box closes.

Adding Global Controllers

You can add up to 63 upstream global controllers and 63 downstream global controllers

To add a global controller:

Step 1 From the **Configuration** menu, choose **Global Controllers**.

The Global Controller 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% of the total link limit.

To edit the maximum bandwidth percentage, continue with the instructions in the *section Editing Global Controllers* (on page [9-35](#)).

Step 3 Click **OK**.

Your changes are saved.

The Global Controller Settings dialog box closes.

Editing Global Controllers

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

To edit a global controller:

Step 1 From the **Configuration** menu, choose **Global Controllers**.

The Global Controller Settings dialog box appears.

Step 2 Click in the BW (%) cell of a global controller listing, and enter the maximum percentage of the total link limit that this global controller should carry.

The values in the BW (Mbps) cell change to reflect the new bandwidth limit.

Step 3 Repeat step 2 for other global controllers.

Step 4 Click **OK**.

Your changes are saved.

The Global Controller Settings dialog box closes.

Deleting Global Controllers

You can delete unused global controllers at any time. The Default Global Controller and the Total Link Limit cannot be deleted.

To delete a global controller:

Step 1 From the **Configuration** menu, choose **Global Controllers**.

The Global Controller Settings dialog box appears.

Step 2 Select a global controller.

Step 3 Click  (**Remove**).

If the specified global controller is being used by a subscriber BWC (see *Editing Package Subscriber BWCs* (on page 9-40)), 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 Controller Settings dialog box closes.

Defining Global Controllers in a Dual Link System

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

Alternatively, you can force bandwidth limitations to be applied to the sum of the two links.

Setting Global Controller Bandwidth Limits in a Dual Link System

To define global controllers for a dual link system:

Step 1 From the **Configuration** menu, choose **Global Controllers**.

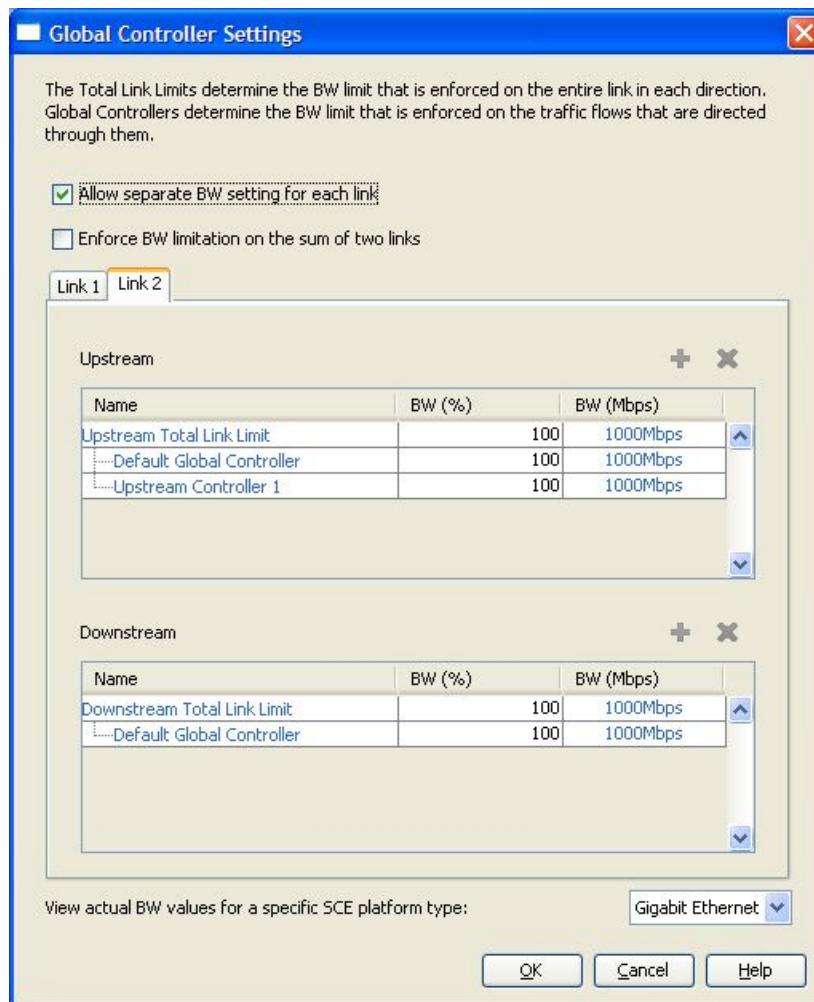
The Global Controller Settings dialog box appears.

Step 2 Check the **Allow separate BW setting for each link** check box.

The dialog box now displays two tabs:

- Link 1
- Link 2

All existing global controllers appear in both tabs; the bandwidth limits are copied from the Link 1 tab to the Link 2 tab.



Step 3 Select the Link 1 tab, and add (see *Adding Global Controllers* (on page 9-34)) and delete (see *Deleting Global Controllers* (on page 9-35)) global controllers as required.

Global controllers can only be added or deleted in the Link 1 tab. All such changes in the Link 1 tab are automatically copied to the Link 2 tab.

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

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

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

Step 6 Click **OK**.

Your changes are saved.

The Global Controller Settings dialog box closes.

Setting Bandwidth Limits as the Sum of Two Links

To set single bandwidth limits in a dual link system:

Step 1 From the **Configuration** menu, choose **Global Controllers**.

The Global Controller Settings dialog box appears.

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

The bandwidth value in each cell in the BW (Mbps) column of the global controller lists is doubled.

Step 3 Click **OK**.

Your changes are saved.

The Global Controller Settings dialog box closes.

Managing Subscriber Bandwidth

Once you have defined global controllers, you can add subscriber BWCs to packages and map these subscriber BWCs to different global controllers.

A *Subscriber BWC* is a mechanism that supports the control of subscriber bandwidth consumption for upstream or downstream flows. A BWC enables the control and metering of 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.

There are two *Primary BWCs* that operate at the subscriber level, one for upstream traffic and one for downstream traffic. The Primary BWCs allocate bandwidth to specific subscribers, depending upon the Committed Information Rate (CIR), 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 the two Default BWCs. This enables the BWC mechanism to control rate sub-partitioning within the Default BWC rate control, based on the CIR, PIR, CoS, 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 *Defining Per-Flow Actions for a Rule* (on page 9-14).
- An *Extra BWC* is a unique capability that also operates at the subscriber level. Extra BWCs are allocated for services that are not included in the Primary BWC. Extra BWCs are defined (based on CIR, PIR, Global Controller, and AL), in addition to the Primary BWC. An Extra BWC should be defined for services that are not often used but have strict bandwidth requirements, for example, a video conference call. 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.

Bandwidth Control is explained in greater detail in the section *Subscriber Bandwidth Control* (on page 3-12).

Subscriber BWC Parameters

The following are the configuration parameters in the Subscriber BW Controllers tab of the Package Settings dialog box:

- Name—A unique name for each BWC.
- CIR—The minimum bandwidth that must be granted to traffic that is controlled by the BWC.
- PIR—The maximum bandwidth allowed to traffic that is controlled by the BWC.


- **Global Controller**—The global controller with which this subscriber BWC is associated. The global controllers are virtual queues that are part of the bandwidth control mechanism (see *Global Bandwidth Control* (on page 3-12)). Traffic with similar bandwidth control properties should be directed to the same global controller.
- **AL**—How fast bandwidth decreases from PIR to CIR as congestion builds, or increases from CIR to PIR as congestion decreases. A higher AL ensures a higher bandwidth compared to a similar BWC with a lower AL. 1 is the lowest assurance value, 10 (persistent) is the highest assurance value.

Assurance Level 10 (persistent) has the added quality that it does not ever reduce below the relevant CIR, unless the total line rate cannot sustain this.

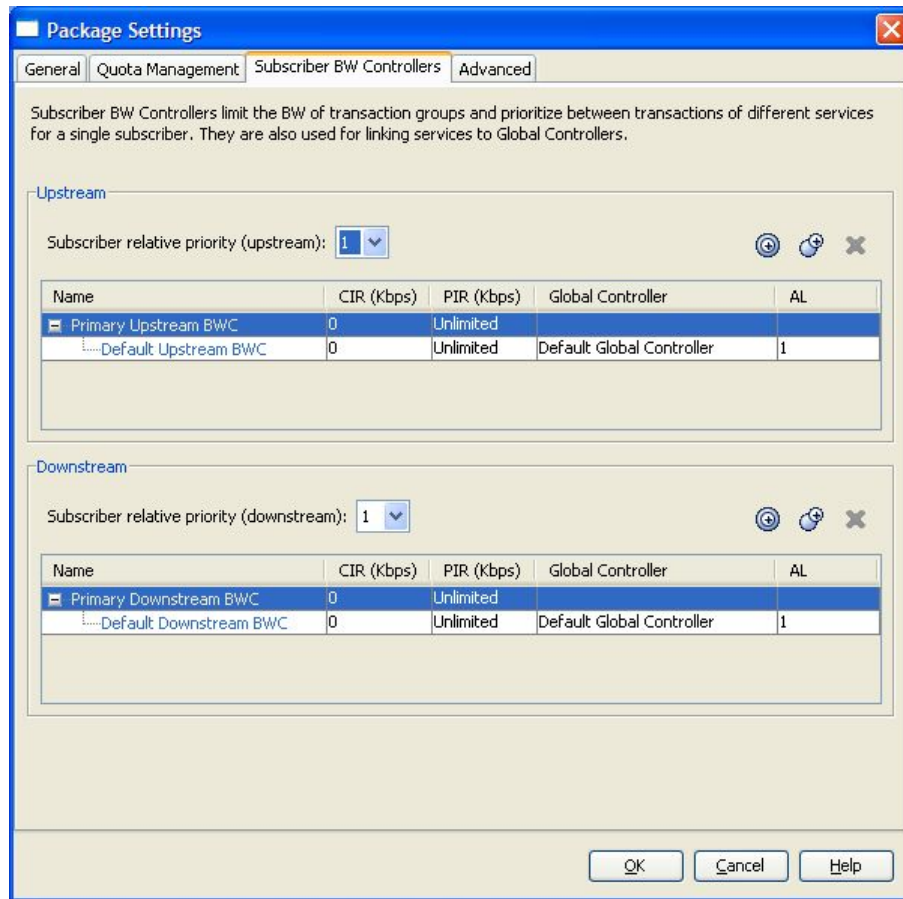
- **Subscriber relative priority**—Assurance Level given to the Total BWC of the subscriber. It determines the assurance given to all the subscriber traffic when competing for bandwidth with subscribers to other packages. 1 is the lowest value and 10 is the highest value.

Editing Package Subscriber BWCs

To edit the package BWC settings:

-
- Step 1** In the Network Traffic tab, select a package from the package hierarchy.
 - Step 2** In the Network Traffic tab, click  (**Edit Package**).
The Package Settings dialog box appears.
 - Step 3** In the Package Settings dialog box, click the **Subscriber BW Controllers** tab.

The Subscriber BW Controllers tab of the Package Settings dialog box appears.



Step 4 Set your requirements for upstream bandwidth control in the Upstream area of the dialog box:

a) Select a value from the Subscriber relative priority drop-down list.

1 is the lowest priority and 10 is the highest.

b) To add a BWC to the package, click (Add a sub BW Controller). Repeat as required.

c) To add an Extra BWC to the package, click (Add an extra BW Controller). Repeat as required.

d) Set the parameters to required values for each BWC (including the Primary and Default BWCs):

- 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
- Select a controller from the Global Controller drop-down list
- Select a value from the AL drop-down list

1 is the lowest value and Persistent is the highest value

Step 5 Repeat step 4 for downstream bandwidth control in the Downstream area of the dialog box.

Step 6 Click **OK**.

The Package Settings dialog box closes.

All changes to the BWC settings are saved.

Managing Bandwidth: a Practical Example

This section explains how to combine the global controllers and subscriber BWCs to achieve effective bandwidth control.

To configure total bandwidth control:

Step 1 Configure the necessary global controllers.

Try to ascertain which services are likely to be problematic, and what the maximum percentage of total bandwidth should be for each. Services and packages that are not likely to be problematic do not have to be specifically configured and can be included 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 Committed Information Rate (CIR) and the Peak Information Rate (PIR) accordingly.
- b) Select an appropriate global controller for each subscriber BWC.

Step 3 Create a rule for each service that is to have its own BWC.

Select appropriate upstream and downstream BWCs for each service.

For example, to limit P2P and streaming traffic:

This example assumes that the traffic flow is bidirectional; you may decide that you only need upstream controllers *or* downstream controllers.

Step 1 Define two upstream global controllers and two downstream global controllers; assign the desired percentage of traffic to each global controller.

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.

The screenshot shows the 'Link 1' configuration window in the SCE. It is divided into two main sections: 'Upstream' and 'Downstream'. Each section contains a table with columns for 'Name', 'BW (%)', and 'BW (Mbps)'. Below the tables, there is a dropdown menu to 'View actual BW values for a specific SCE platform type:' set to 'Gigabit Ethernet'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Name	BW (%)	BW (Mbps)
Upstream Total Link Limit	100	1000Mbps
.....Default Global Controller	100	1000Mbps
.....Upstream Controller 1	20	200Mbps
.....Upstream Controller 2	25	250Mbps

Name	BW (%)	BW (Mbps)
Downstream Total Link Limit	100	1000Mbps
.....Default Global Controller	100	1000Mbps
.....Downstream Controller 1	20	200Mbps
.....Downstream Controller 2	25	250Mbps

View actual BW values for a specific SCE platform type: Gigabit Ethernet

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

Managing Bandwidth

(BWC1 is for upstream P2P traffic and BWC3 is for downstream P2P traffic; BWC2 is for upstream streaming traffic and BWC4 is for downstream streaming traffic.)

Package Settings

General Quota Management **Subscriber BW Controllers** Advanced

Subscriber BW Controllers limit the BW of transaction groups and prioritize between transactions of different services for a single subscriber. They are also used for linking services to Global Controllers.

Upstream

Subscriber relative priority (upstream): 1

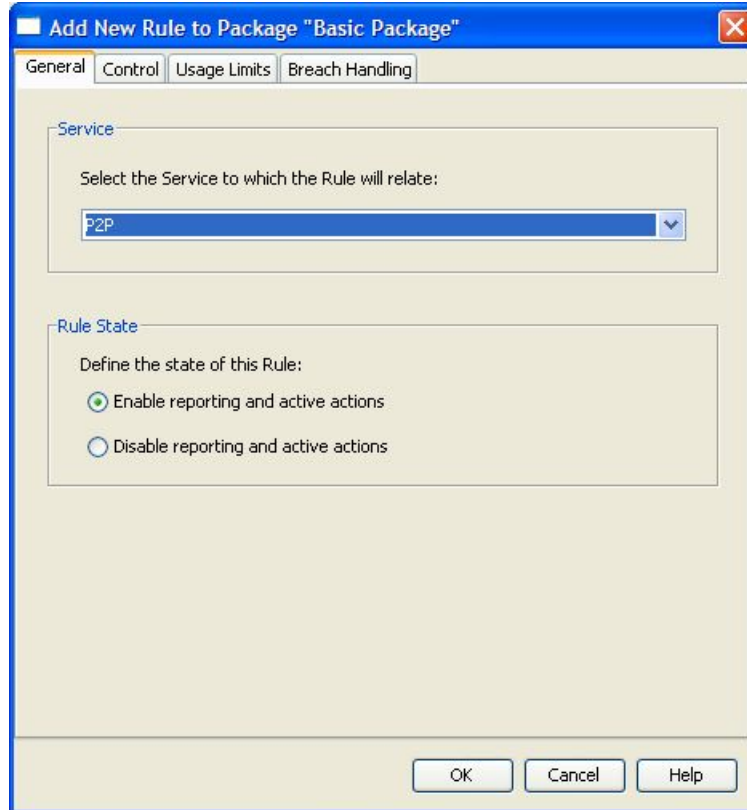
Name	CIR (Kbps)	PIR (Kbps)	Global Controller	AL
Primary Upstream BWC	0	Unlimited		
Default Upstream BWC	0	Unlimited	Default Global Controller	1
BWC 1	0	Unlimited	Upstream Controller 1	1
BWC 2	0	Unlimited	Upstream Controller 2	1

Downstream

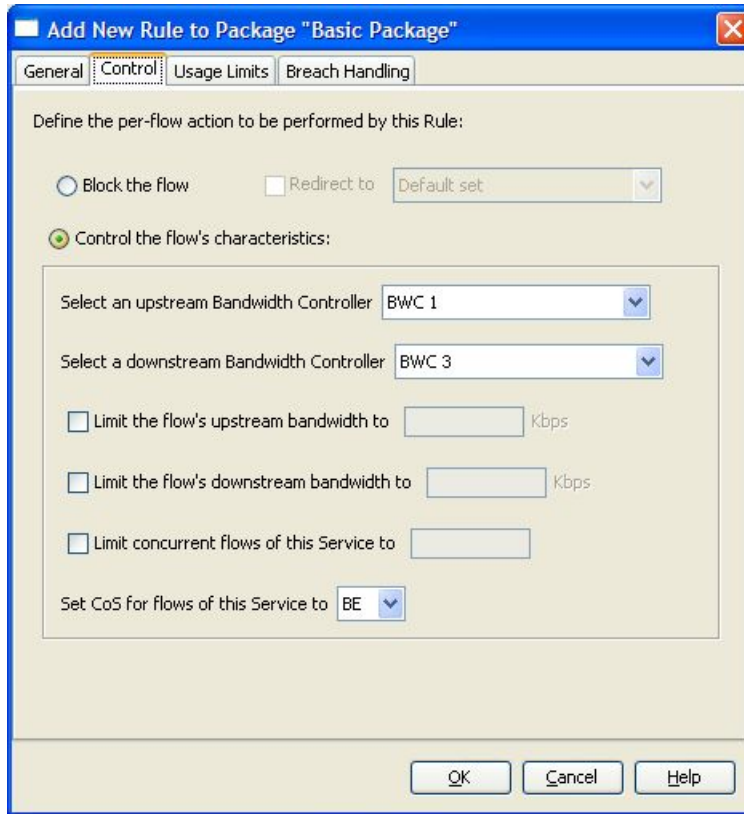
Subscriber relative priority (downstream): 1

Name	CIR (Kbps)	PIR (Kbps)	Global Controller	AL
Primary Downstream BWC	0	Unlimited		
Default Downstream BWC	0	Unlimited	Default Global Controller	1
BWC 3	0	Unlimited	Downstream Controller 1	1
BWC 4	0	Unlimited	Downstream Controller 2	1

OK Cancel Help

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 and BWC 4.

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

Setting BW Management Prioritization Mode

Relative priority is the level of assurance that internal BWCs get when competing against other internal BWCs for bandwidth. There are two relative priority options:

- Global Prioritization Mode—Flows that go through internal BWCs get their relative priority from the BWC's assurance level.
- Subscriber Prioritization Mode (default)—The relative priority of the flow is determined by the relative priority of the subscriber.

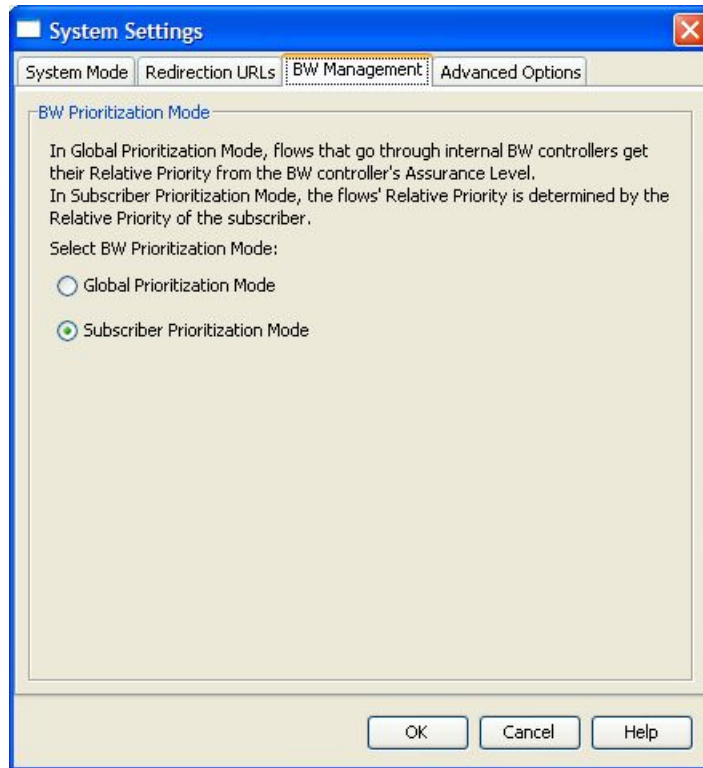
To set the BW Management parameters:

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

The System Settings dialog box appears.

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

The BW Management tab of the System Settings dialog box appears.



Step 3 Click 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 Quotas

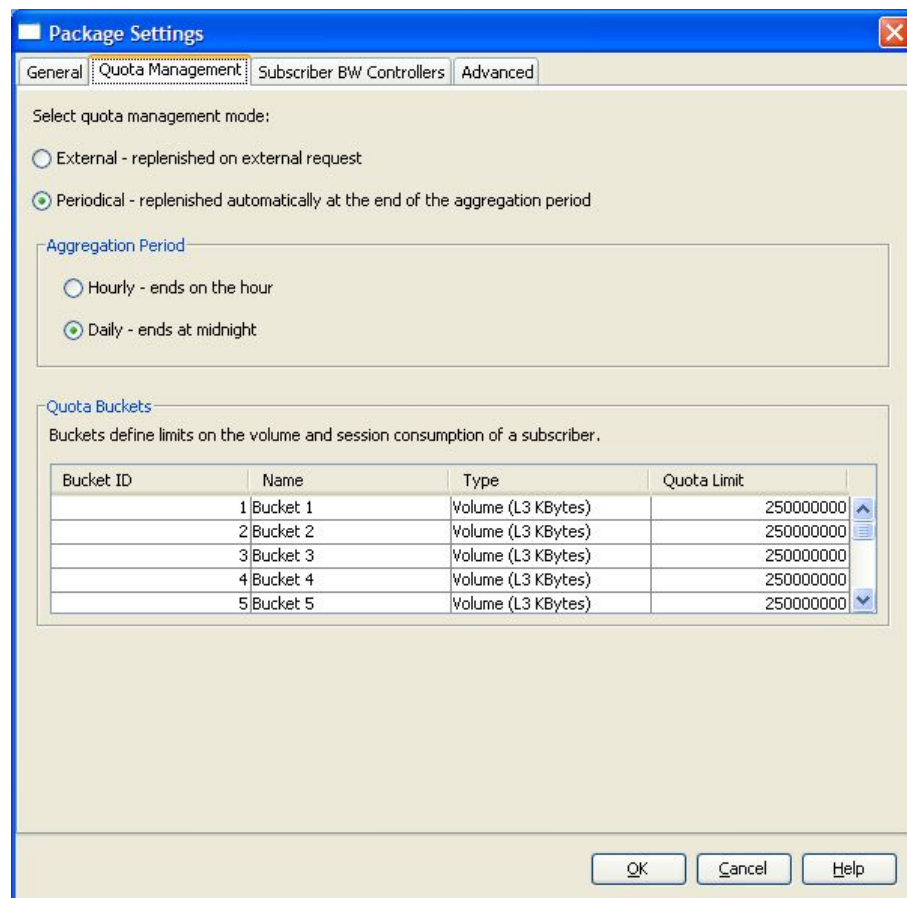
Editing Package Quota Management Settings

You can define whether quota management is performed by an external quota manager, or by *SCA BB*.

You also define the quota buckets associated with the package. Quota buckets can be used by rules to set limits to consumption of particular service groups (see the following section).

To edit the package quota management settings:

-
- Step 1** In the Network Traffic tab, select a package from the package hierarchy.
 - Step 2** In the Network Traffic tab, click  (**Edit Package**).
 - The Package Settings dialog box appears.
 - Step 3** In the Package Settings dialog box, click the **Quota Management** tab.
 - The Quota Management tab of the Package Settings dialog box appears.



- Step 4** Select the quota management mode by clicking a **quota management mode** radio button:

- **External**—Replenished on external request
- **Periodical**—Replenished automatically

Step 5 If you selected periodical quota management, click one of the **Aggregation Period** radio buttons to specify when the quota is renewed for the package:

- **Hourly Resolution**—Ends at each hour change
- **Daily Resolution**—Ends at midnight

Step 6 Configure the quota buckets. Make sure that the configuration of the quota buckets 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.

To edit a bucket:

- **Bucket ID**—*Display only.*
- **Name**—Enter a name for the bucket in the Name cell

The default name for the protocol can be used; it is recommended that you enter a meaningful name

- **Type**—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
- **Quota Limit**—Define the actual limit for this bucket in Kbytes or number of sessions, depending on the selected Type

Quota limits can only be set if you selected periodical quota management in step 4

Step 7 Click **OK**.

The Package Settings dialog box closes.

All changes to the quota management settings are saved.

Selecting Quota Buckets for Rules

The Usage Limits tab is used to select the quota buckets to be used by the flows mapped to this rule. The quota buckets in the drop-down lists were defined during package setup (see *Editing Package Quota Management Settings* (on page 9-48)). If no quota bucket is appropriate for the rule, add a new quota bucket to the package, or edit an existing bucket.

To select quota buckets for a rule:

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

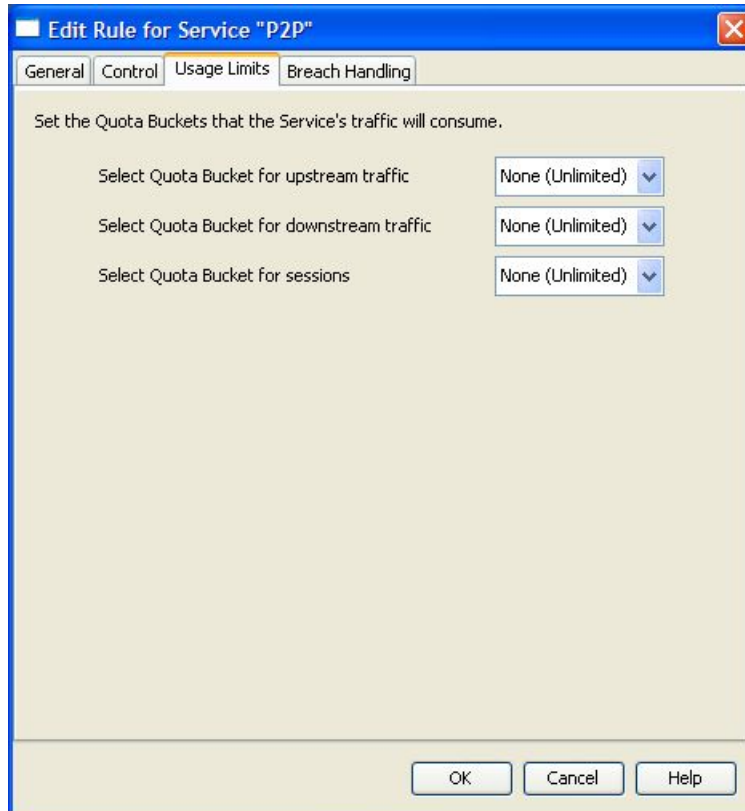
Step 2 In the Rule pane, select a rule.

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

The Edit Rule for Service dialog box appears.

Step 4 Click the **Usage Limits** tab.

The Usage Limits tab of the Edit Rule for Service dialog box appears.



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**

Select "None (Unlimited)" for unlimited quota.

Step 6 To define behavior when a quota is breached, if you have selected a quota bucket for any for the options in step 5, continue with the instructions in the following section, *Editing Breach Handling Parameters for a Rule* (on page 9-51).

Step 7 Click **OK**.

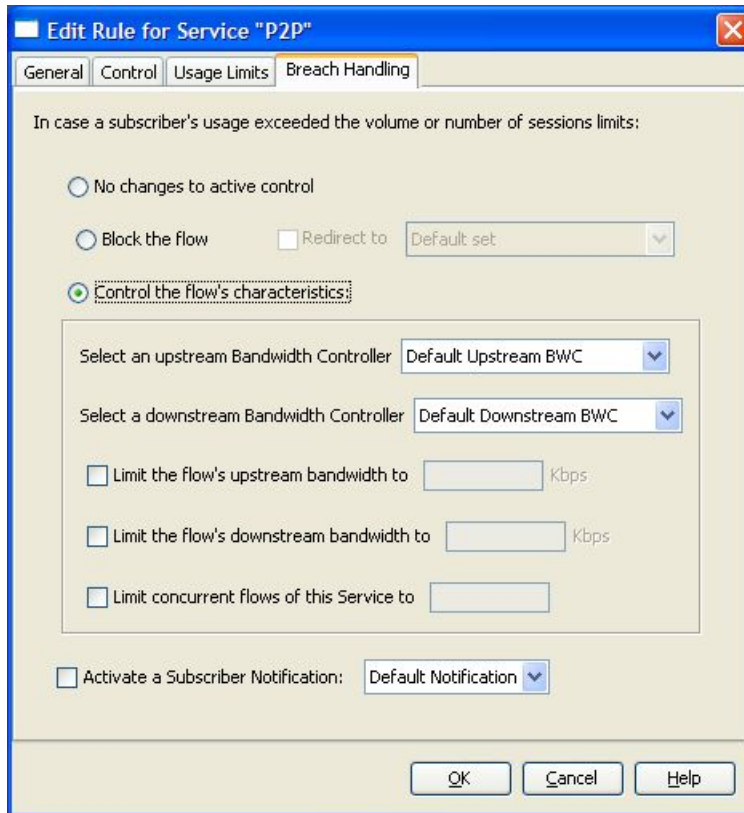
The Edit Rule for Service dialog box closes.

All changes to the rule are saved.

Editing Breach Handling Parameters for a Rule

The Breach Handling tab of the Edit Rule for Service dialog box allows you to change 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.

When you select the **Breach Handling** tab, the following dialog box appears.



The dialog box has three sections. In the upper section you determine what happens to flows identified as belonging to this rule when a quota has been breached:

- **No changes to active control**—Selecting this option means that flows mapped to this rule are not affected when quota is breached. Quota Breach RDRs can be generated even when this option is selected (see *Managing Quota RDRs* (on page 8-6)).
- **Block the flow**—When you select this radio button, the Redirect option is enabled:
 - **Redirect to**—If you check the **Redirect to** check box, the Redirection URL Set drop-down list is enabled. From this drop-down list, select the URL set that is to serve as the redirection target. URL redirection sets are defined in the System Settings dialog box. (See *Configuring the Redirection Parameters* (on page 10-19).) Only three protocol types support redirection: HTTP, HTTP Streaming, and RTSP.
- **Control the flow characteristics**—When you select this radio button the options in the central area of the dialog box are enabled:

- **Select an upstream Bandwidth Controller**—The BWCs in this drop-down list are defined when creating or editing the package (see *Editing Package Subscriber BWCs* (on page 9-40)). Use this option to map this rule's traffic flows to a specific upstream BWC. This sets up bandwidth metering of all concurrent flows mapped to this rule, based on the characteristics of the selected BWC.

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

- **Select a downstream Bandwidth Controller**—The same functionality as the previous option, but for downstream flow.
- **Limit the flow's upstream bandwidth**—Used to set a per-flow upstream bandwidth limit (for flows mapped to the service of this rule).
- **Limit the flow's downstream bandwidth**—Used to set a per-flow downstream bandwidth limit.
- **Limit concurrent flows of this Service**—Use this option to set the maximum number of concurrent flows (mapped to this rule) permitted to a subscriber.
- **Activate a Subscriber Notification**—Use this option to select a previously defined Subscriber Notification (see *Managing Subscriber Notifications* (on page 10-9)) that will be activated when subscribers exceed their quota limit. This notification could, for example, convey the quota breach situation to the subscriber and provide information on how to obtain additional quota.

Subscriber Notification may be activated with any of the options for breach-handling behavior.

To define breach-handling behavior for the rule:

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

Step 2 In the 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 of the Edit Rule for Service dialog box appears.

Step 5 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, click the **No changes to active control** radio button.

Step 6 Continue at step 10.

Step 7 To block flow's that are mapped to the service of this rule:

- a) Click the **Block the flow** radio button

The Redirect check box is enabled.

- b) (Optional) To redirect blocked flows (for HTTP, HTTP Streaming, and RTSP), check the **Redirect to** check box.

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** to continue.

- c) Select a redirection URL set from the Redirect drop-down list.

Step 8 Continue at step 10.

Step 9 Click 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
- From the downstream Bandwidth Controller drop-down list, select a downstream BW Controller
- (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 **Limit concurrent flows of this Service** check box and enter a value in the associated field

Step 10 (Optional) Activate subscriber notification:

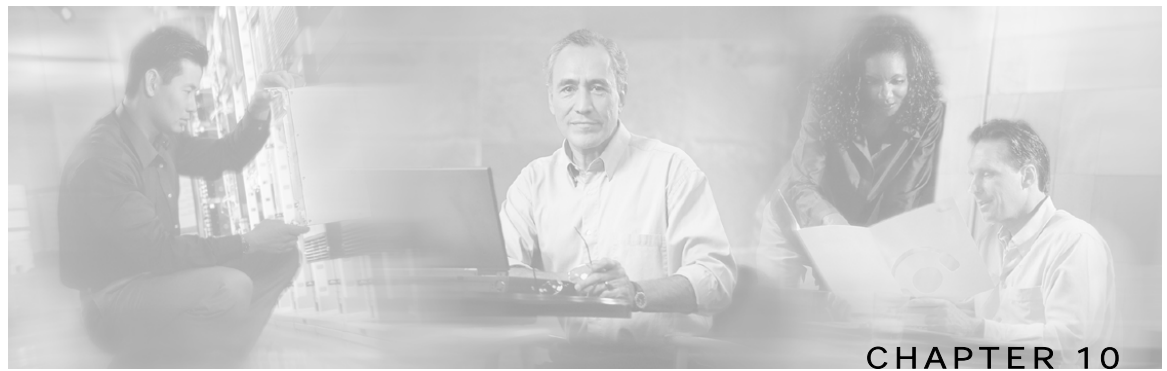
- Check the **Activate a Subscriber Notification** check box and then select the desired subscriber notification from the drop-down list.

A subscriber notification can be activated in addition to any of the three breach-handling options.

Step 11 Click **OK**.

The Edit Rule for Service dialog box closes.

All changes to the rule are saved.



Using the Service Configuration Editor: Additional Options

This chapter explains how to use additional, advanced functionality that is available in the Service Configuration Editor.

This chapter contains the following sections:

- [Filtering the Traffic Flows](#) 10-1
- [Managing Subscriber Notifications](#) 10-9
- [Managing the System Settings](#) 10-14
- [Managing VAS Traffic Forwarding Settings](#) 10-23

Filtering the Traffic Flows

Filter rules are part of the service configuration. They allow you to instruct the Service Control Engine (SCE) platform to ignore some types of flow based on the flow's Layer 3 and Layer 4 properties, and transmit the flows unchanged.

When a traffic flow enters the SCE platform, the platform checks whether a filter rule applies to this flow.

If a filter rule does apply 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 within any records generated for analysis purposes nor will the flows 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) which might traverse the SCE platform - these protocols usually should not be affected by policy enforcement; also they are of low volume, and insignificant for reporting.

A number of filter rules are included in every new service configuration.



Note

Some of the predefined filter rules are, by default, active by while others are deactivated.

Viewing Filter Rules

You can view a list of the filter rules included in the service configuration.

The listing for each filter rule includes the name of the rule, its status, and a brief description of the rule (generated by the system).

To see more information about a filter rule, open the Edit Filter Rule dialog box (see *Editing Filter Rules* (on page 10-7)).

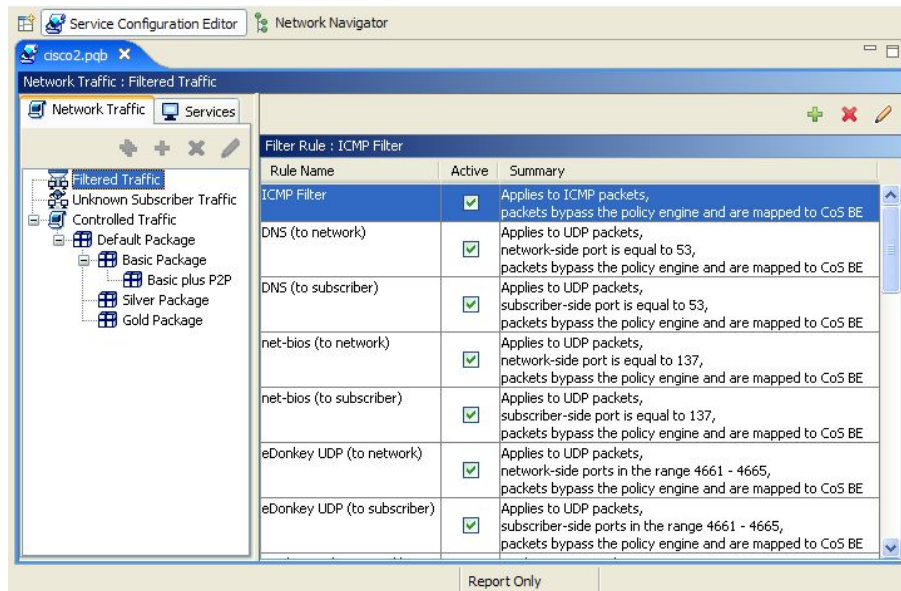
To view the rules for a package:

Step 1 In the current service configuration, click the **Network Traffic** tab.

The Network Traffic tab appears.

Step 2 In the Network Traffic tab, select the **Filtered Traffic** node.

A list of all filter rules appears in the Rule pane.



Adding Filter Rules

The Add Filter Rule Wizard guides you through the process of adding a filter rule.

To add a filter rule:

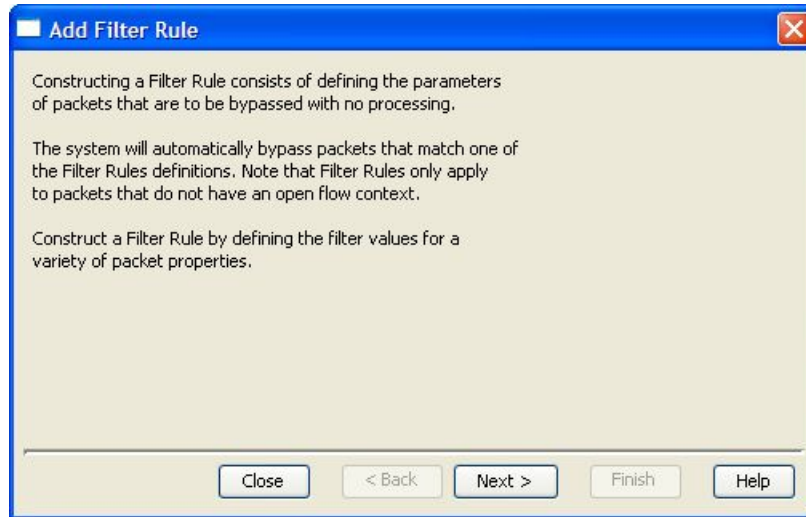
Step 1 In the current service configuration, click the **Network Traffic** tab.

The Network Traffic tab appears.

Step 2 In the Network Traffic tab, select the **Filtered Traffic** node.

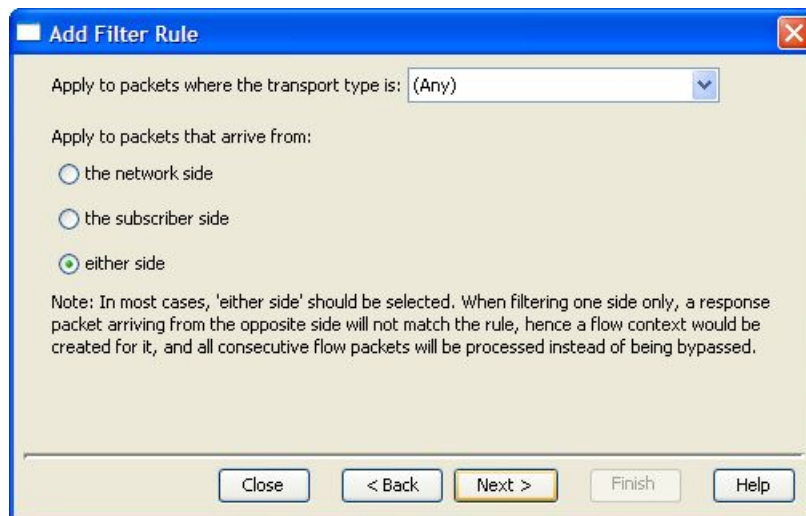
Step 3 Click **+** (**Add Rule**) in the Rule pane.

The Add Filter Rule Wizard - Start dialog box appears.



Step 4 Click **Next**.

The Add Filter Rule Wizard - Protocol dialog box appears.



Step 5 Select the transport type and initiating side, and click **Next**.

The Add Filter Rule Wizard - Source IP Address dialog box appears.

The screenshot shows a dialog box titled "Add Filter Rule" with a close button (X) in the top right corner. The main text reads "Apply to packets where the subscriber-side IP address is:". Below this, there are five radio button options, each with a corresponding text input field:

- Any IP address
- Equal to
- Other than
- In the range of -
- Not in the range of -

At the bottom of the dialog box, there are five buttons: "Close", "< Back", "Next >" (highlighted in yellow), "Finish", and "Help".

Step 6 Define the source IP address and click **Next**.

The Add Filter Rule Wizard - Destination IP Address dialog box appears.

The screenshot shows a dialog box titled "Add Filter Rule" with a close button (X) in the top right corner. The main text reads "Apply to packets where the network-side IP address is:". Below this, there are five radio button options, each with a corresponding text input field:

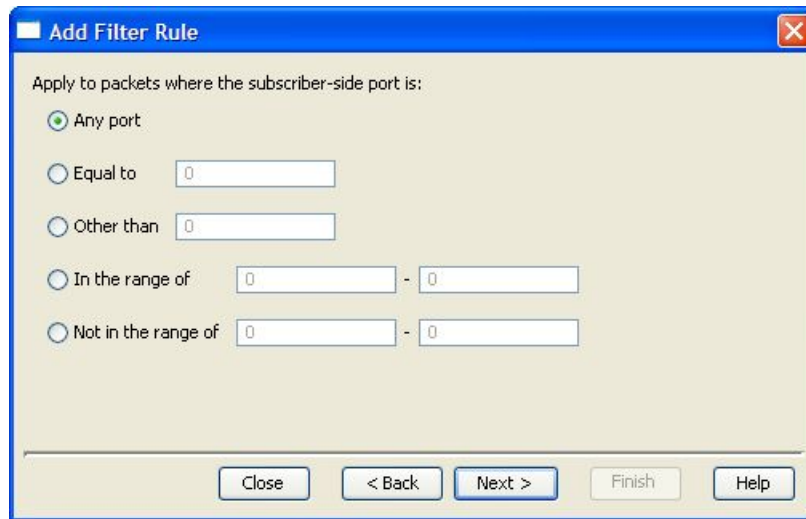
- Any IP address
- Equal to
- Other than
- In the range of -
- Not in the range of -

At the bottom of the dialog box, there are five buttons: "Close", "< Back", "Next >" (highlighted in blue), "Finish", and "Help".

Step 7 Define the destination IP address and click **Next**

If the transport protocol selected was TCP, UDP or ANY, the Add Filter Rule Wizard - Source Port dialog box appears.

If any other transport protocol was selected, the Add Filter Rule Wizard - ToS dialog box appears. Go to step 9.



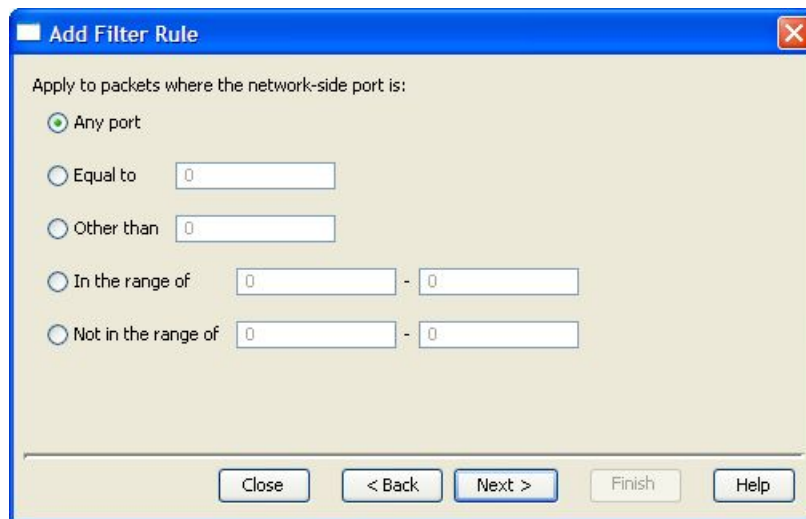
The screenshot shows a dialog box titled "Add Filter Rule" with a close button (X) in the top right corner. The main text reads "Apply to packets where the subscriber-side port is:". Below this, there are five radio button options, each followed by a text input field containing the number "0":

- Any port
- Equal to 0
- Other than 0
- In the range of 0 - 0
- Not in the range of 0 - 0

At the bottom of the dialog box, there are five buttons: "Close", "< Back", "Next >", "Finish", and "Help". The "Next >" button is highlighted with a blue border.

Step 8 Define the source port and click **Next**.

The Add Filter Rule Wizard - Destination Port dialog box appears.



The screenshot shows a dialog box titled "Add Filter Rule" with a close button (X) in the top right corner. The main text reads "Apply to packets where the network-side port is:". Below this, there are five radio button options, each followed by a text input field containing the number "0":

- Any port
- Equal to 0
- Other than 0
- In the range of 0 - 0
- Not in the range of 0 - 0

At the bottom of the dialog box, there are five buttons: "Close", "< Back", "Next >", "Finish", and "Help". The "Next >" button is highlighted with a blue border.

Step 9 Define the destination port and click **Next**

The Add Filter Rule Wizard - ToS dialog box appears.

The screenshot shows the 'Add Filter Rule' dialog box with the following configuration:

- Title: Add Filter Rule
- Instruction: Apply to packets where the ToS is:
- Selected option: Any value
- Other options:
 - Equal to: [0]
 - Other than: [0]
 - In the range of: [0] - [0]
 - Not in the range of: [0] - [0]
- Buttons: Close, < Back, Next >, Finish, Help

Step 10 Define the ToS and click **Next**.

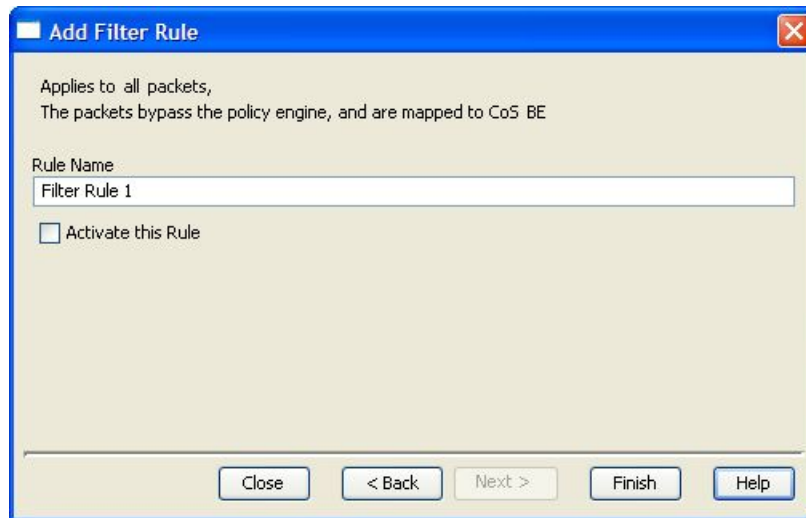
ToS acceptable values are 0-63.

The Add Filter Rule Wizard - CoS dialog box appears.

The screenshot shows the 'Add Filter Rule' dialog box with the following configuration:

- Title: Add Filter Rule
- Text 1: The system automatically bypasses packets if their properties match this filter's definitions.
- Text 2: The system maps the bypassed packets to a certain Class-of-Service.
- Label: Select the CoS to use:
- Value: BE (dropdown menu)
- Buttons: Close, < Back, Next >, Finish, Help

Step 11 Select the CoS value and click **Next**. The Add Filter Rule Wizard - Finish dialog box appears.



Step 12 In the Rule Name field, enter a unique name for the new filter rule.

The default name for the filter rule can be used; it is recommended that you enter a meaningful name.

(Optional) Check the **Activate this rule** check box to activate the filter rule. Traffic is filtered according to the rule only when it is activated.

Step 13 Click **Finish**.

The filter rule is added and displayed in the Filter Rule table.

Editing Filter Rules

You can view and edit the parameters of a filter rule.

To edit a filter rule:

Step 1 In the current service configuration, click the **Network Traffic** tab.

The Network Traffic tab appears.

Step 2 In the Network Traffic tab, select the **Filtered Traffic** node.

A list of all filter rules appears in the Rule pane.

Step 3 Select a rule in the Filter Rule table.

Step 4 Click  (**Edit Rule**).

The Edit Filter Rule Wizard - Start dialog box appears.

The Edit Filter Rule Wizard is the same as the Add Filter Rule Wizard.

Step 5 Follow the instructions in the section *Adding Filter Rules* (on page 10-2), step 4 through step 11.

Step 6 Click **Finish**.

The filter rule is changed; relevant changes are made in the Filter Rule table.

Deleting Filter Rules

Filter rules can be deleted; 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.

To delete a filter rule:

Step 1 In the current service configuration, click the **Network Traffic** tab.

The Network Traffic tab appears.

Step 2 In the Network Traffic tab, select the **Filtered Traffic** node.

A list of all filter rules appears in the Rule pane.

Step 3 Select a rule in the Filter Rule table.

Step 4 Click  (**Remove Rule**).

A Filter Rule Warning message appears.



Step 5 Click **Yes**.

The filter rule is deleted and is no longer displayed in the Filter Rule table.

Activating and Deactivating 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 the filter rule can be reactivated at a later date.

To change the status of a filter rule:

-
- Step 1** In the current service configuration, click the **Network Traffic** tab.
The Network Traffic tab appears.
 - Step 2** In the Network Traffic tab, select the **Filtered Traffic** node.
A list of all filter rules appears in the Rule pane.
 - Step 3** Select a rule in the Filter Rule table.
 - Step 4** To activate the rule, check the **Active** check box.
 - Step 5** To deactivate the rule, uncheck the **Active** check box.
 - Step 6** Repeat steps 2 to 4 as required.
-

Managing Subscriber Notifications

The subscriber notification feature provides the means to push 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.

Subscriber notifications during a network attack are described in *Attack Filtering and Subscriber Notification* (on page 13-5).

The *Cisco Service Control Application for Broadband (SCA BB)* supports a maximum of 31 subscriber notifications, including the Default Notification.

Subscriber Notification Parameters

A subscriber notification is defined by the following parameters:

- Name—Each service must have a unique name.
- Destination URL—Once redirection is activated, HTTP flows of the subscriber are redirected to a configurable destination URL. 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 numeric ID of the notification that redirected the subscriber and <subscriber-ID> is the subscriber name.

These parameters can be used by the destination web server to carry a more purposeful message to the subscriber.

- Dismissal method—Indicates when to dismiss, or deactivate, the notification state. May be any one of the following:
 - Subscriber browses to destination URL (default)—As soon as subscribers browse to the destination URL, they are considered to have been notified and the notification state is dismissed

For example, if subscribers have exceeded their quota, the notification state is dismissed as soon as they browse to the destination URL, which informs them of this fact (even though the subscribers would still remain 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 instance, if subscribers have exceeded their quota, the notification state may only be dismissed when they have completed the procedure to refresh their quota
 - Subscriber browses to dismissal URL—The subscriber must proceed from the destination URL to a different final URL before the notification state is dismissed

All HTTP flows are redirected until the notification is dismissed. The notification is dismissed when the subscriber accesses the dismissal URL. By default, the destination URL is also the dismissal URL, so a notification is dismissed once the first redirection takes place. However, it is possible to define a different dismissal URL, so that the subscriber must acknowledge the notification.

For instance, if subscribers have exceeded their quota, 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> [ * ]
```



Note

The path element must always start with '/'.

- <hostname> may optionally be preceded by a wildcard (*), to match all hostnames with the same suffix.
- <path> may be followed by a wildcard, to match all paths with common prefix.

For example, the entry:

```
*.some-isp.net:/redirect/*
```

matches all these 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.

Once 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 can be useful, for example, to give subscribers access to additional support information.

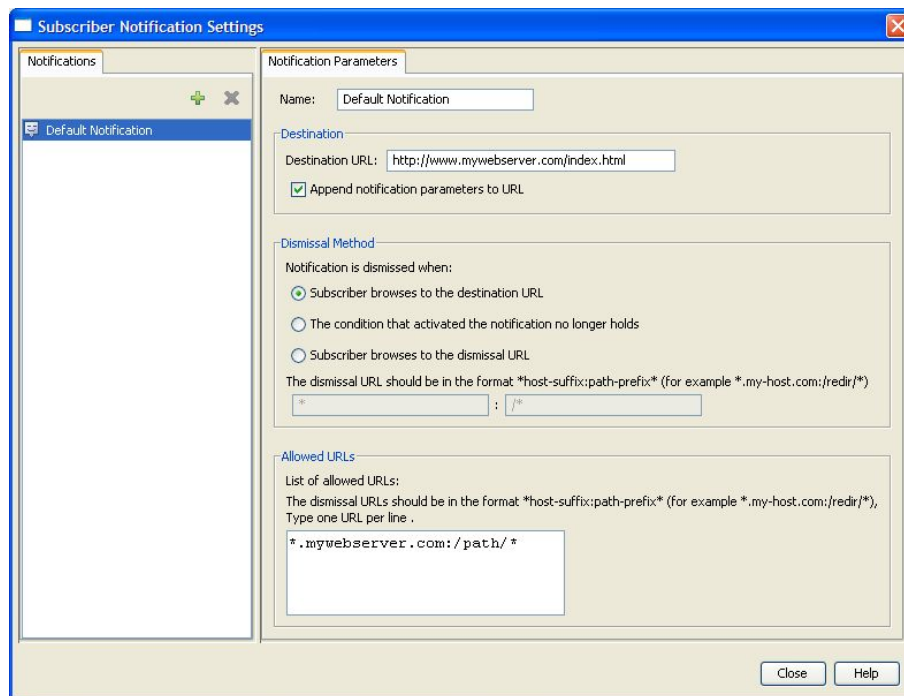
Allowed URLs have the same format as the dismissal URL.

These parameters are defined when you add a new subscriber notification (see *Adding Subscriber Notifications* (on page 10-12)), and can be changed at any time (see *Editing Subscriber Notifications* (on page 10-13)).

Viewing Subscriber Notifications

Step 1 From the **Configuration** menu, choose **Subscriber Notifications**.

The Subscriber Notifications Settings dialog box appears.



The Notifications tab displays a list of all subscriber notifications.

Step 2 Click on 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.

Adding Subscriber Notifications

You can add up to 30 subscriber notifications to a service configuration.

To add a subscriber notification:

Step 1 From the **Configuration** menu, choose **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.

The default name for the subscriber notification can be used; 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 are to be appended to the destination URL, check the **Append notification's parameters to URL** check box.

Step 6 Select the dismissal method by clicking a **Dismissal Method** radio button:

- **Subscriber browses to the destination URL**
- **The condition that activated the notification no longer holds**
- **Subscriber browses to the dismissal URL**
 - (Optional) Enter the dismissal URL host-suffix and path-prefix in the fields provided

Step 7 Enter any allowed URLs, one per line, in the Allowed URLs text box.

Step 8 Click **Close**.

The Subscriber Notifications Settings dialog box closes.



Note

The creation of 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 *Editing Breach Handling Parameters for a Rule* (on page 9-51).)

Editing Subscriber Notifications

You can modify notification parameters at any time.


To edit a subscriber notification:

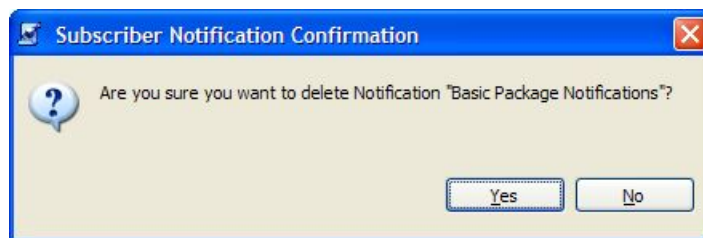
-
- Step 1** From the **Configuration** menu, choose **Subscriber Notifications**.
The Subscriber Notifications Settings dialog box appears.
 - Step 2** Click on a subscriber notification in the Notifications tab to display its parameters.
 - Step 3** Edit the parameters of the subscriber notification in the Notification Parameters tab.
 - Step 4** Click **Close**.
The Subscriber Notifications Settings dialog box closes.
-

Deleting Subscriber Notifications

You can delete subscriber notifications at any time. You cannot delete the Default Notification.

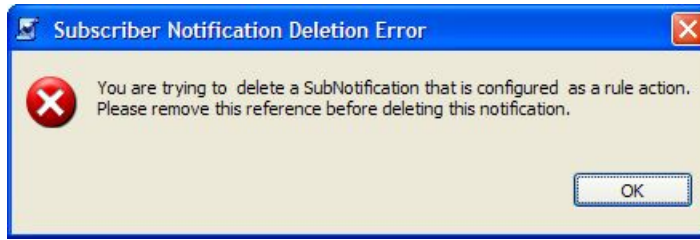
To delete a subscriber notification:

-
- Step 1** From the **Configuration** menu, choose **Subscriber Notifications**.
The Subscriber Notifications Settings dialog box appears.
 - Step 2** Click on a subscriber notification in the Notifications tab.
 - Step 3** Click  (**Remove**).
A Subscriber Notification Confirmation message appears.



- Step 4** Click **Yes**.

- If the specified subscriber notification is being used by a rule (see *Editing Breach Handling Parameters for a Rule* (on page 9-51)), a Subscriber Notification Deletion Error message is displayed.



The subscriber notification cannot be deleted until you unassign it or deactivate it in all service rules.

The selected subscriber notification is deleted.

Step 5 Click **Close**.

The Subscriber Notifications Settings dialog box closes.

Managing the System Settings

The SCAS BB Console allows you to determine various system parameters that control:

- The operational state of the system
- The redirection URLs for protocols that support redirection
- BW prioritization mode (see *Setting BW Management Prioritization Mode* (on page 9-46))
- Advanced service configuration options

Setting the Operational Mode of the System

The SCAS BB Console allows you to select the operational mode of the system. This feature defines how the system handles network traffic.



Note

Rules have an enabled/disabled mode of their own, which might differ from the system mode. In this case, 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 System Modes are:

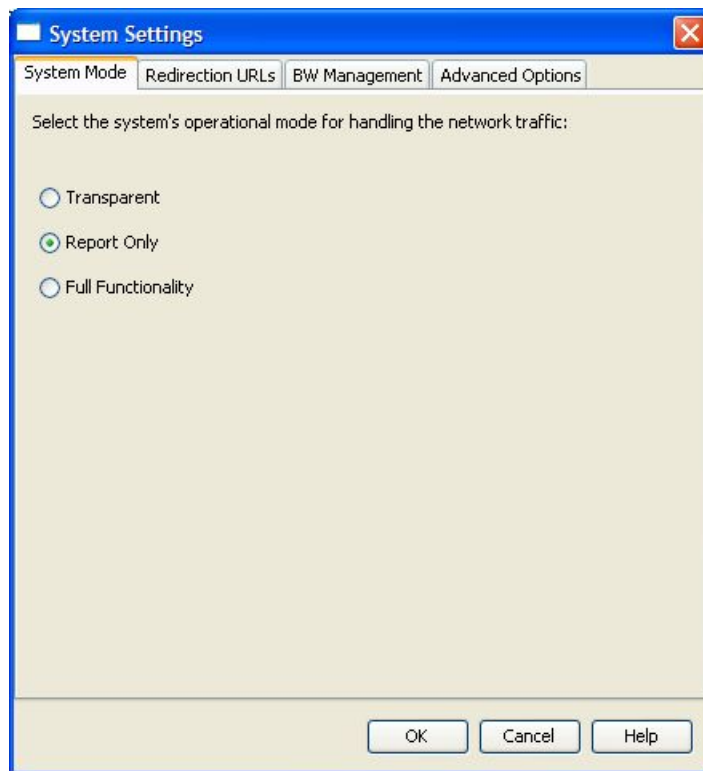
- **Full Functionality**—The system performs reporting, as well as active network enforcement according to the defined settings and rules.

- **Report Only**—The system performs reporting functions only (that is, generates RDRs) according to the system settings and rule definitions. No active rule enforcement is performed on the network traffic. In this mode, the report-only status is assigned to all rules in the entire system; the report option functions for analysis or debug purposes only; for example, to report when specified limitations are reached. No active networking enforcements are performed, meaning that the rule parameters are not enforced by the SCE platforms.
- **Transparent**—The system does not generate RDRs and does not enforce active rules on the network traffic.

To configure the system mode parameter:

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

The System Settings dialog box appears.



Step 2 Click one of the **operational mode** buttons:

- **Full functionality**
- **Reports only**
- **Transparent**

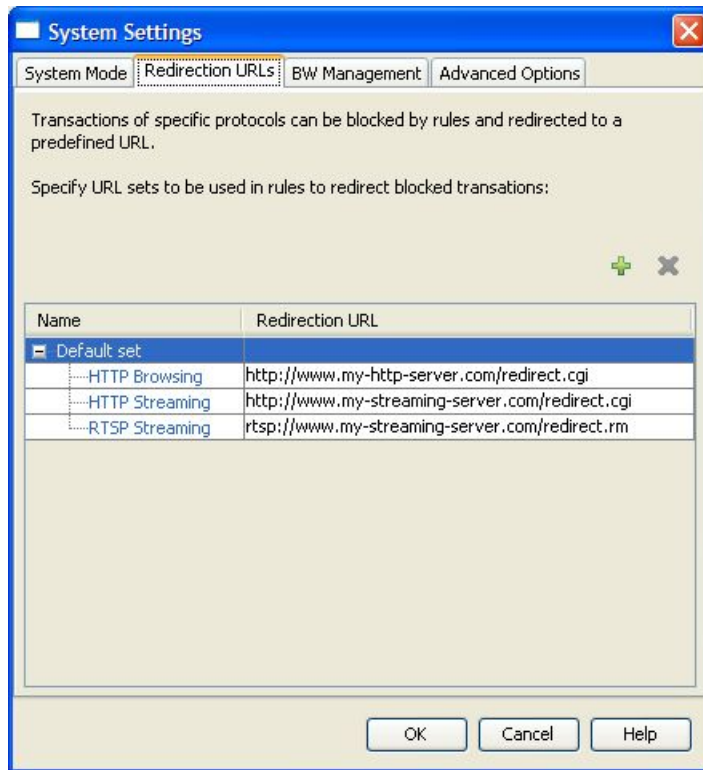
Step 3 Click **OK**.

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 protocol that is blocked, the traffic flow is redirected to an appropriate URL. Different blocked protocols are redirected to different URLs. This feature is configured when defining rules (see *Defining Per-Flow Actions for a Rule* (on page 9-14)).



These sets of *redirection URLs* are defined in the Redirection URLs tab of the System Settings dialog box.

Use the SCAS BB Console Redirection feature to define the URL to which specific types of protocols will be redirected. Not all protocols are supported. The three protocols that are supported are:

- HTTP Browsing
- HTTP Streaming
- RTSP Streaming

Each set of redirection URLs contains one redirection option for each of these three protocols.

The system provides a default set of redirection URLs. This set cannot be deleted. You can add additional sets, giving each a significant name. When generating a new set, the system automatically supplies the current default URL values. You can assign a different URL to each protocol, or use the same URL supplied under the default set of redirection URLs.

Each redirection URL includes the URL specified name, the Subscriber ID and the Service ID, set in the following format:

```
<URL>?n=<subscriber-ID>&s=<service-ID>
```

One possible use of this feature is to redirect subscribers to a server where a posted web page provides them with an explanation that includes details on the cause for the redirection. The reason may be, for example, a "Silver" subscriber trying to access a service that is only available to "Gold" subscribers. It is possible to use this web page to then offer subscribers the opportunity to upgrade their packages.

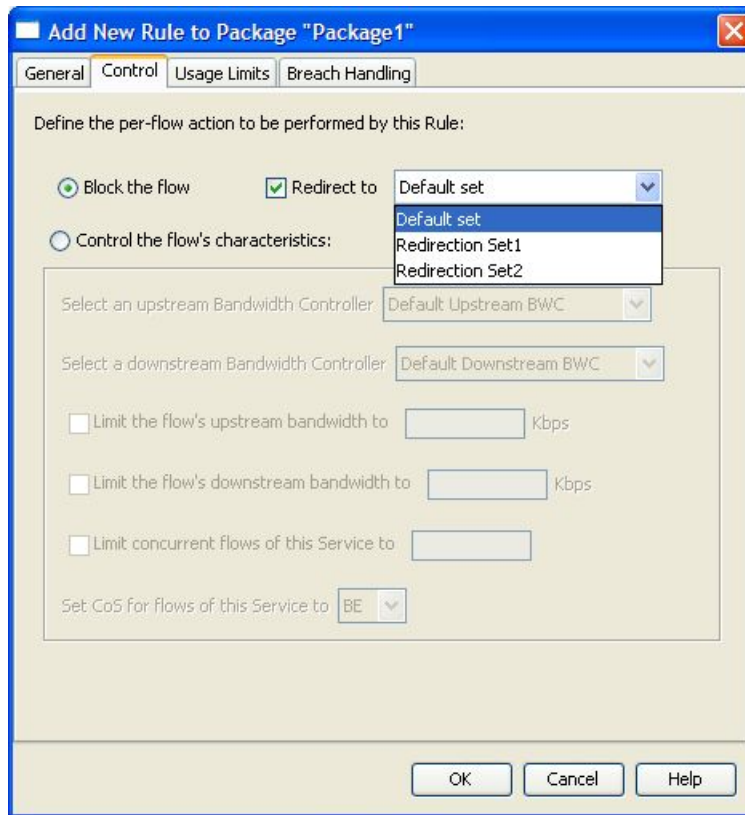
Adding a Set of Redirection URLs

You can add up to 49 redirection sets.

To add a redirection set:

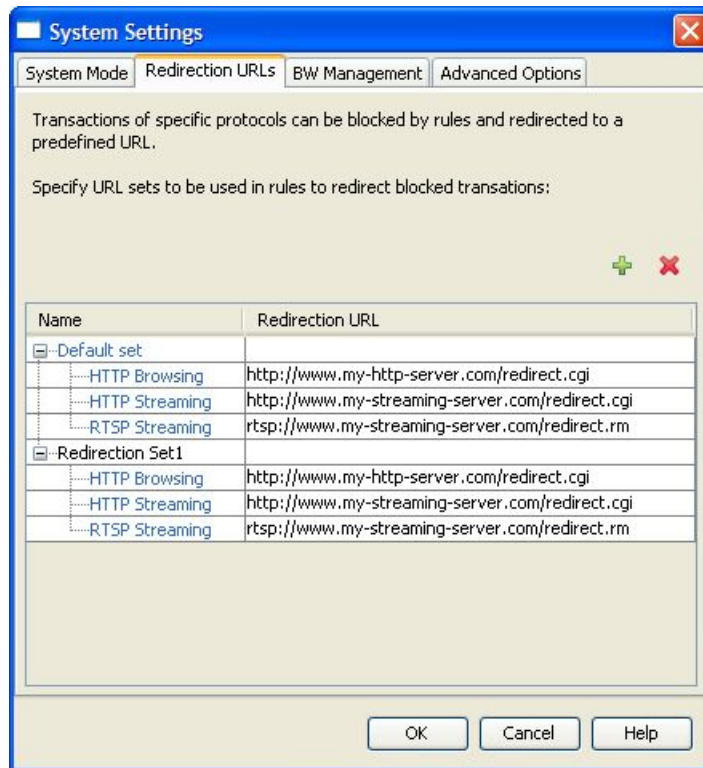
-
- Step 1** From the **Configuration** menu, choose **System Settings**.
The System Settings dialog box appears.
 - Step 2** Click the **Redirection URLs** tab.

The Redirection URLs tab of the System Settings dialog box appears.



Step 3 Click **+** (Add).

A new redirection set appears containing the default redirection URLs.



Step 4 In the Name field, enter a unique name for the new redirection set.

The default name for the redirection set can be used; it is recommended that you enter a meaningful name.

Step 5 (Optional) 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.

Configuring the Redirection Parameters

To edit an existing set of Redirection URLs:

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

The System Settings dialog box appears.

Step 2 Click the **Redirection URLs** tab.

The Redirection URLs tab of the System Settings dialog box appears.

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.

Deleting a Set of Redirection URLs

To delete a redirection set:

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

The System Settings dialog box appears.

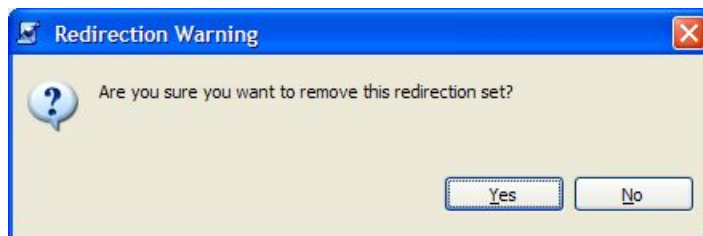
Step 2 Click the **Redirection URLs** tab.

The Redirection URLs tab of the System Settings dialog box appears.

Step 3 Click a redirection set name.

Step 4 Click  (**Remove**).

A Redirection Warning message appears.



Step 5 Click **Yes**.

The redirection set is deleted.

Step 6 Click **OK**.

The System Settings dialog box closes.

Managing Advanced Service Configuration Options

Advanced service configuration options control the more sophisticated and less frequently changed attributes of the system. It is recommended not to change these options.

The following table lists these options:

Property	Default Value	Description
Classification: UDP ports for which flow should be opened on first packet	5060, 5061, 67, 69, 1812, 1813, 1645, 1646, 2427, 2727, 9201, 9200	Enhanced flow-open mode is disabled on the specified UDP ports, to allow classification according to the flow's first packet
Policy Check: Ongoing policy check mode active	True	Whether policy changes affect flows that are already open
Policy Check: 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 This period should be used by a policy server to provision quota to a subscriber that just logged in
Quota Management: 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
Quota Management: 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 0 means that unlimited volume may pass

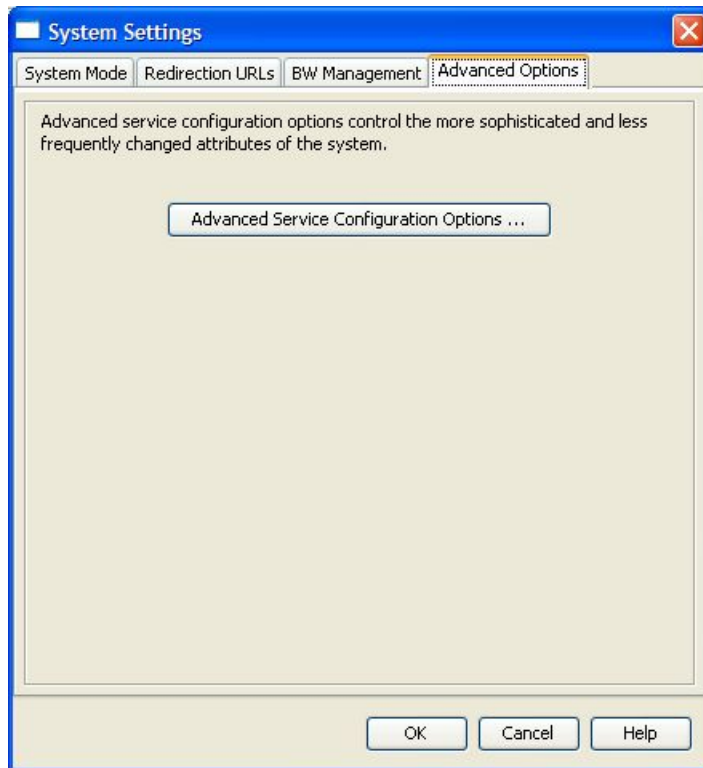
Editing Advanced Service Configuration Options

To edit the advanced service configuration options:

-
- Step 1** From the **Configuration** menu, choose **System Settings**.
The System Settings dialog box appears.
- Step 2** Click the **Advanced Options** tab.

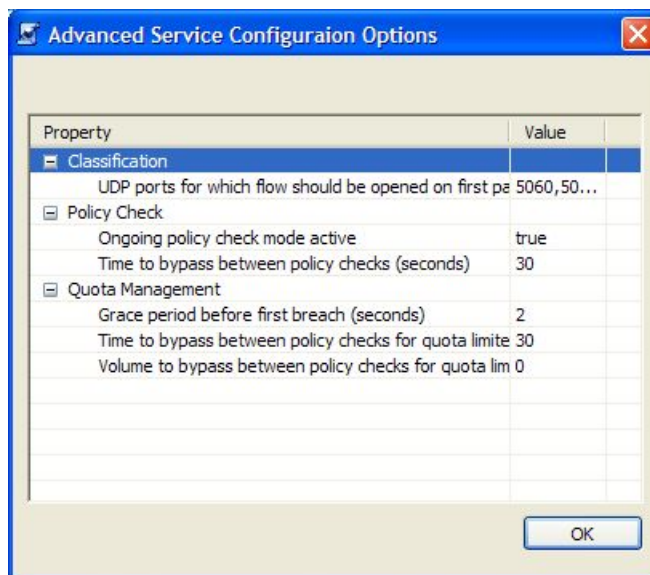
Managing the System Settings

The Advanced Options tab of the System Settings dialog box appears.



Step 3 Click **Advanced Service Configuration Options**.

The Advanced Service Configuration Options dialog box appears.



Step 4 Make any required 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:

- VAS traffic forwarding is supported on the SCE 2000 4xGBE platform only
- A single SCE platform can support up to eight VAS servers
- There can be a maximum of 64 traffic forwarding tables in a service configuration
- There can be a maximum of 64 table parameters in a traffic forwarding table

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 in the *Cisco Service Control Engine Software Configuration Guide*.

VAS Traffic Forwarding and Bandwidth Management

Due to the complexity of the VAS traffic forwarding feature, some SCE platform bandwidth management capabilities change when VAS traffic forwarding is enabled:

- VAS flows are not subject to global BW control
- The number of global controllers available to regular flows is decreased

Global Controllers and VAS Flows

When VAS traffic forwarding is enabled, the global controllers function slightly differently:

- The number of global controllers available to the user is reduced from 64 to 48
- Global controllers 48 to 63 are used to count VAS traffic
- Any flows that are configured to global controllers 48 to 63 will be attached to the default global controller

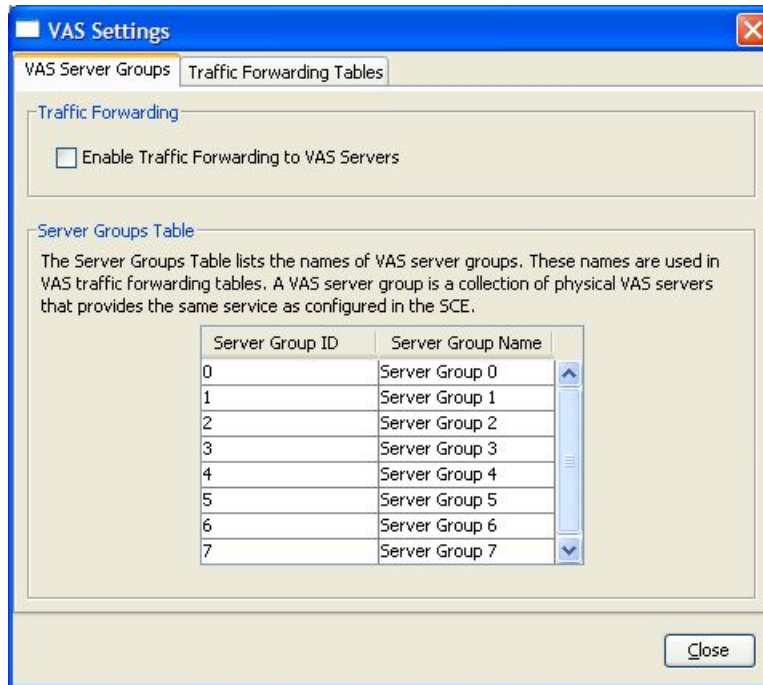
Enabling VAS Traffic Forwarding

By default, VAS traffic forwarding is disabled; you can enable it at any time.

To enable VAS traffic forwarding:

Step 1 From the **Configuration** menu, choose **VAS Settings**.

The VAS Settings dialog box appears.



Step 2 Check the **Enable Traffic Forwarding to VAS Servers** check box.

The VAS Traffic Forwarding Table drop-down list in the Advanced tab of the Package Settings dialog box is enabled (see *Setting Advanced Package Options* (on page 9-6)).

Step 3 Click **Close**.

The VAS Settings dialog box closes.

To disable VAS traffic forwarding:

Step 1 From the **Configuration** menu, choose **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.

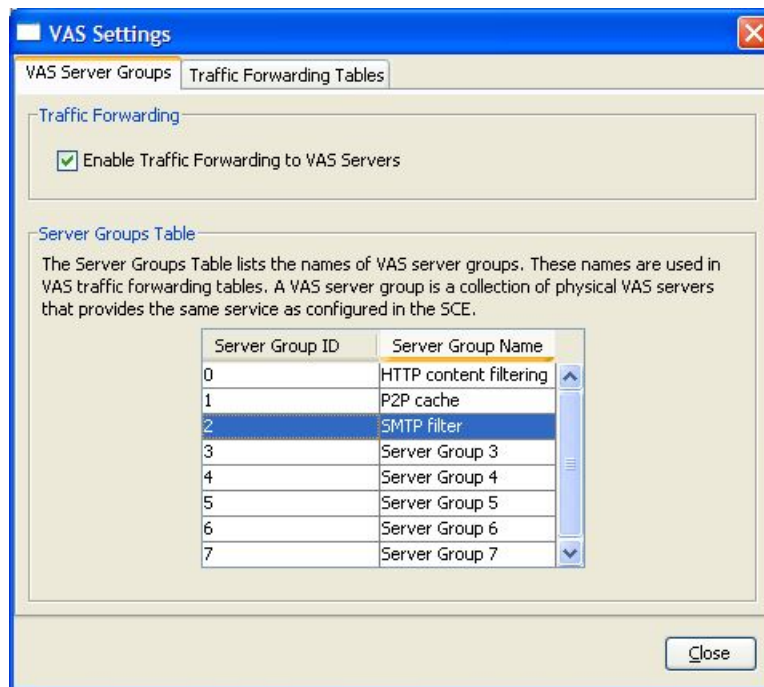
Renaming VAS Server Groups

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. You should 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 *Setting Advanced Package Options* (on page 9-6)) and in the Server Group field of the table parameters added to each traffic forwarding table (see *Managing VAS Table Parameters* (on page 10-28)).

To rename VAS server groups:

Step 1 From the **Configuration** menu, choose **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.

Viewing 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.

To view VAS traffic forwarding tables:

Step 1 From the **Configuration** menu, choose **VAS Settings**.

The VAS Server Groups tab of the VAS Settings dialog box appears.

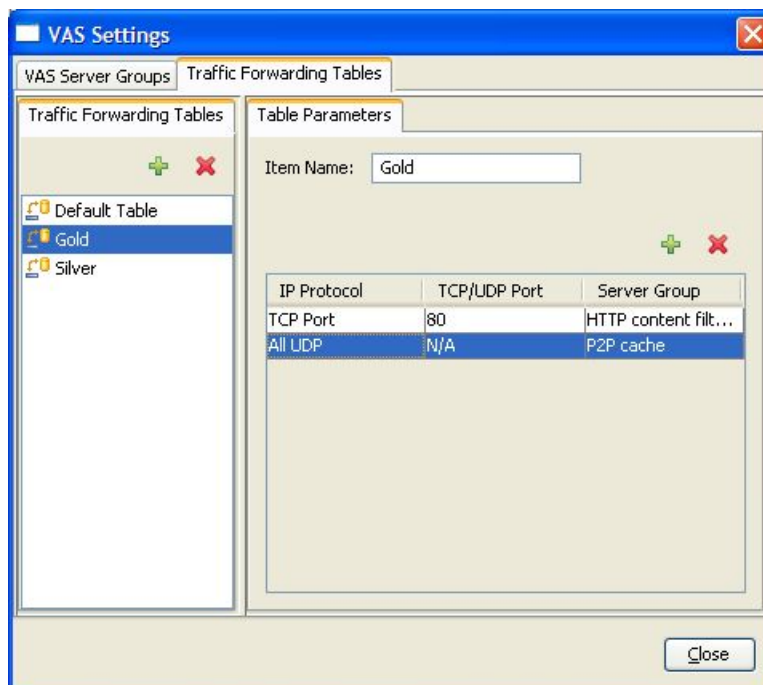
Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab of the VAS Settings dialog box appears.

A list of all existing traffic forwarding tables is displayed in the Traffic Forwarding Tables area.

Step 3 Click on a table in the traffic forwarding tables list to display its table parameters.

A list of all table parameters defined for this traffic forwarding table appears in the Table Parameters tab.



Step 4 Click **Close**.

The VAS Settings dialog box closes.

Adding 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.


To add a VAS traffic forwarding table:

Step 1 From the **Configuration** menu, choose **VAS Settings**.

The VAS Server Groups tab of the VAS Settings dialog box appears.

Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab of the VAS Settings dialog box appears.

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 also appears 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.

Step 5 You can now add tables parameters to the new traffic forwarding table, see *Adding VAS Table Parameters* (on page [10-28](#)).

Deleting VAS Traffic Forwarding Tables

All user-created traffic forwarding tables can be deleted. (The default traffic forwarding table cannot be deleted.)



Note A traffic forwarding table associated with a package cannot be deleted.

To delete a VAS traffic forwarding table:

Step 1 From the **Configuration** menu, choose **VAS Settings**.

The VAS Server Groups tab of the VAS Settings dialog box appears.

Step 2 Click the **Traffic Forwarding Tables** tab.

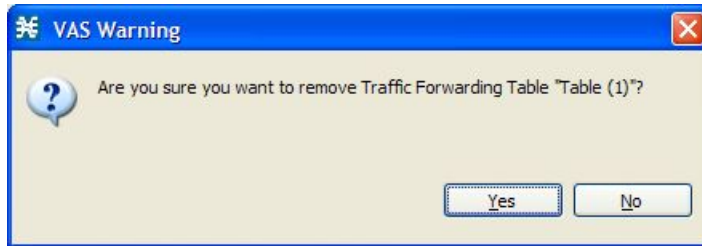
The Traffic Forwarding Tables tab of the VAS Settings dialog box appears.

Managing VAS Traffic Forwarding Settings

Step 3 From the list of traffic forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 4 Click  (**Remove**).

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.

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.

- There can be a maximum of 64 table parameters per traffic forwarding table

Adding VAS Table Parameters

You can add up to 64 table parameters to a traffic forwarding table.

To add a VAS traffic forwarding table:

Step 1 From the **Configuration** menu, choose **VAS Settings**.

The VAS Server Groups tab of the VAS Settings dialog box appears.

Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab of the VAS Settings dialog box appears.

Step 3 From the list of traffic forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 4 In the Table Parameters tab, click  (**Add**).

A new table parameter is added to the list of table parameters in the Table Parameters tab.

Each new table parameter has default values of: IP Protocol = TCP Port, TCP/UDP Port = 80, Server Group = Server Group 0.

Step 5 You can now edit the new table parameter, as described in the following section.

Step 6 Click **Close**.

The VAS Settings dialog box closes.

Editing VAS Table Parameters

To edit a VAS traffic forwarding table:

Step 1 From the **Configuration** menu, choose **VAS Settings**.

The VAS Server Groups tab of the VAS Settings dialog box appears.

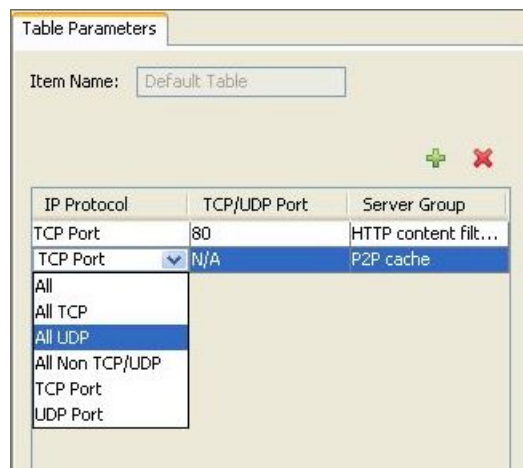
Step 2 Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab of the VAS Settings dialog box appears.

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:

- a) Click in a cell in the IP Protocol column, and, from the drop-down list that opens, select an IP protocol type.

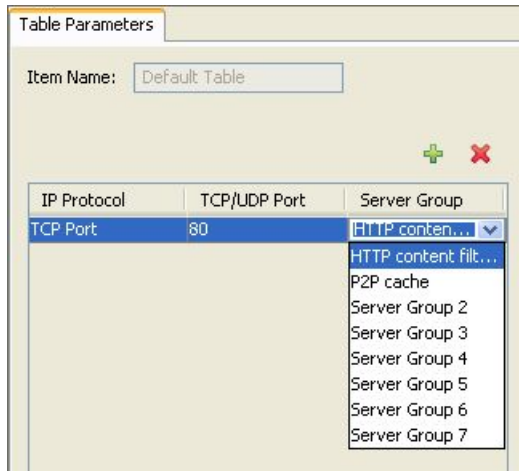


If you select All, All TCP, All UDP, or All Non TCP/UDP, 'N/A' will appear in the TCP/UDP Port cell when you move to another cell in the table.

- b) If you selected TCP Port or UDP Port, double-click in the cell in the TCP/UDP Port column, and enter the required port number.

You cannot add 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.

Deleting VAS Table Parameters

To delete a VAS table parameter:

- Step 1** From the **Configuration** menu, choose **VAS Settings**.

The VAS Server Groups tab of the VAS Settings dialog box appears.

- Step 2** Click the **Traffic Forwarding Tables** tab.

The Traffic Forwarding Tables tab of the VAS Settings dialog box appears.

- Step 3** From the list of traffic forwarding tables in the Traffic Forwarding Tables area, select a table.

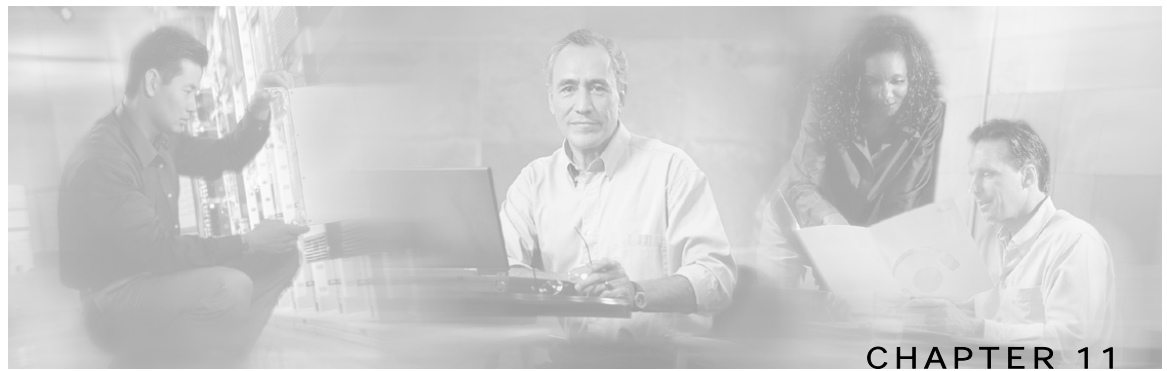
- Step 4** From the list of table parameters in the Table Parameters tab, select a table parameter.

- Step 5** Click **✖ (Remove)**.

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.



Using the Subscriber Manager GUI Tool

This chapter discusses the Subscriber Manager (SM) GUI tool.

The SM GUI tool can be used to configure subscribers on the Cisco Service Control Management Suite (SCMS) Subscriber Manager (SM) database. The SCMS-SM functions as middleware software used to bridge between the OSS and the 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 then be distributed between multiple platforms according to actual subscriber placement.

The SM GUI tool provides only a subset of the functionality that is provided by the SCMS-SM's command-line utilities. For more information about the SCMS-SM, see the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

The *Cisco Service Control Application for Broadband (SCA BB)* can also operate in subscriberless mode, where control and link level analysis functions are provided at a global platform resolution, and anonymous-subscriber mode, where the system dynamically creates "anonymous" subscribers using user-defined IP address ranges as the subscriber name. The SM GUI tool is not applicable for these cases.

This chapter contains the following sections:

- [The SM GUI Tool](#) 11-1
- [Working with Subscriber CSV Files](#) 11-5
- [Managing Subscribers](#) 11-7

The SM GUI Tool

The SM GUI tool allows you to manage subscribers on an SCMS-SM. It is useful when the SCMS-SM holds a static list of subscribers. In addition to importing and exporting the subscriber files, managing subscribers includes 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 *Adding SM Devices to a Site* (on page 5-4)).

Connecting to an SCMS-SM

You can connect to an SCMS-SM:

- From the Network Navigator tool
- From anywhere else in the SCAS BB Console
- From within the Subscriber Manager GUI tool



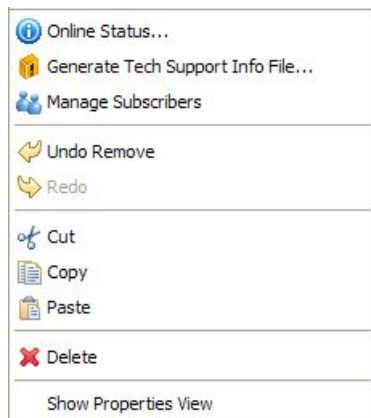
Note

The SM GUI tool performs authentication on the SCMS-SM by opening an FTP connection to port 21, attempting to login as user pcube; if an FTP server with user pcube is not running on the SCMS-SM, authentication will fail.

To connect to an SCMS-SM from the Network Navigator:

Step 1 In the Site Manager tree in the Network Navigator tab, right-click on an SM device.

A short-cut menu appears.



Step 2 From the menu select **Manage Subscribers**.

A Password Management dialog box appears.




Step 3 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

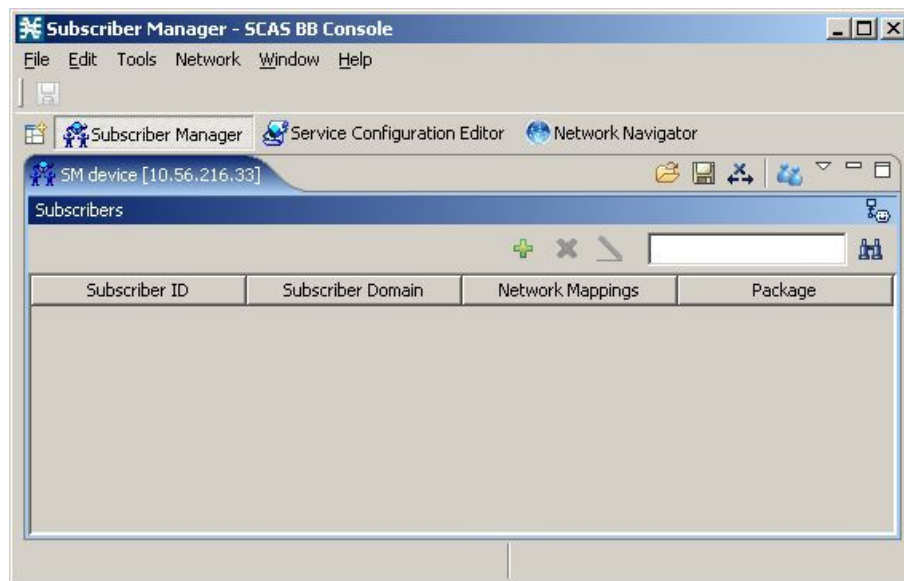
Step 4 Click **Connecting**.

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.



To connect to an SCMS-SM from the SCAS BB Console:

(If you are already in the SM GUI tool, start at step 3.)

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


The SM GUI tool opens.

A Subscriber Manager is not connected message appears.

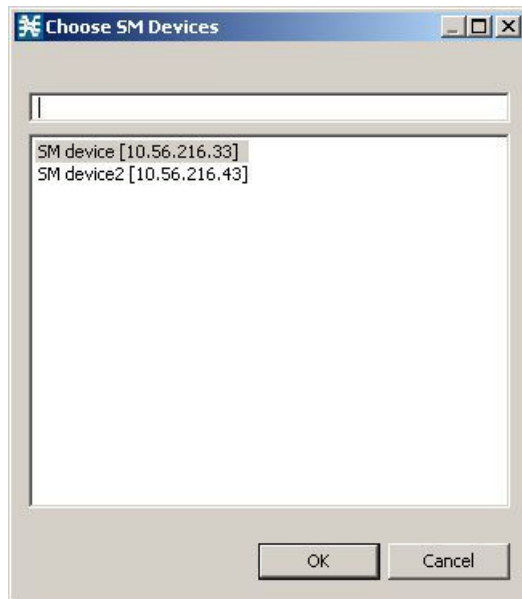


Step 2 Click **OK**.

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 appears.



Step 4 Select a device and click **OK**.

A Password Management dialog box appears.




Step 5 Refer to *Password Management* (on page 5-24) for an explanation of how to fill in the fields.

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.

Disconnecting from an SCMS-SM

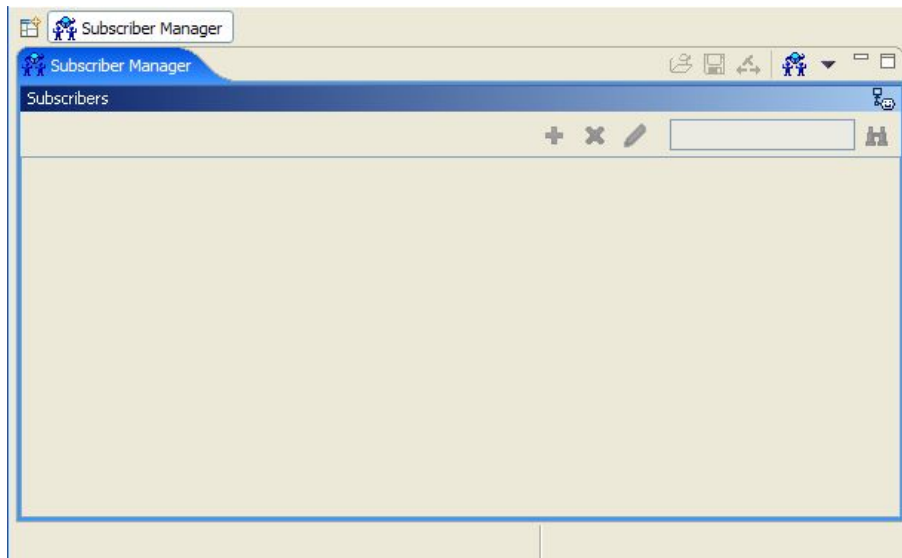
To disconnect from the current SCMS-SM:

In the SM GUI toolbar, click  (**Disconnect from SM**).

The SCAS BB 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

Due to the large number of subscribers that must be introduced into the system, it is not feasible to enter the subscriber information manually. The subscriber information is usually generated by a Radius server (or some similar source) and imported into the SM GUI tool.

It is also possible to export updated subscriber information to a CSV file.

The format of subscriber CSV files is described in the *Cisco Service Control Application for Broadband Reference Guide*.

Importing Subscriber Files

Subscriber data that was exported to a CSV file can be imported into the SM GUI tool.

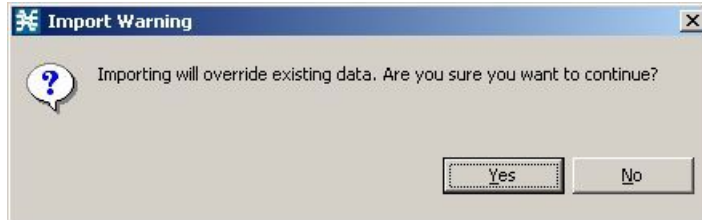
To import subscriber information from a CSV file:

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.

Exporting Subscriber Files

You can export subscriber information to a CSV file (for example, when data in the SCMS-SM database is updated).

To export subscriber information to a CSV file:

Step 1 Select the subscribers whose data you want to save (see *Selecting Subscribers* (on page 11-8)).

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

Once subscribers have been imported into the system, you can maintain and update the database.

You can perform the following operations:

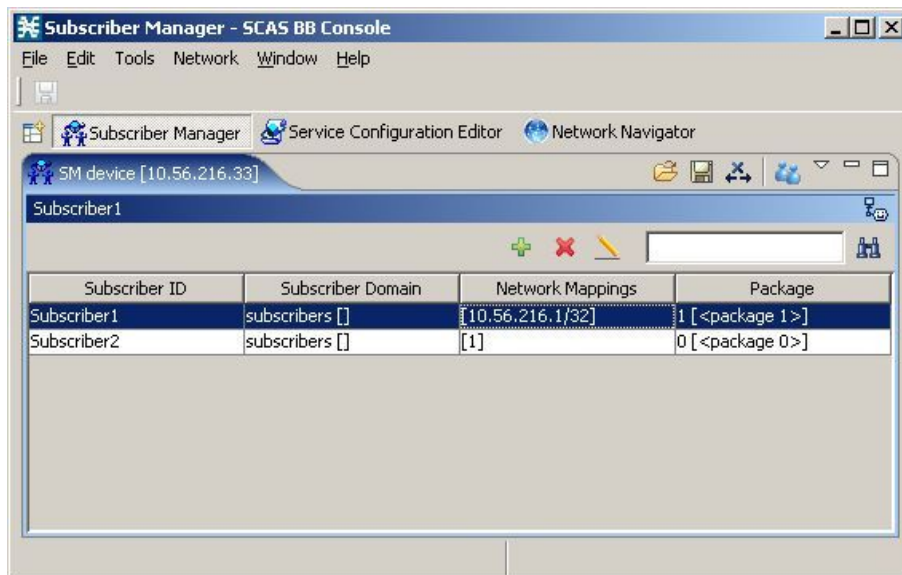
- Add subscribers
- Edit information for existing subscribers
- Delete subscribers

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 *Finding Subscribers* (on page 11-8)).

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 appears in square brackets.



Finding and Selecting Subscribers

For ease of use, the SM GUI tool incorporates two standard features:

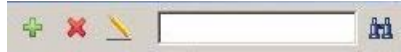
- Find—Search for a specific subscriber
- Multiple Select—Select a range of subscribers or a number of individual subscribers


Finding 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 Subscribers* (on page 11-11)).

To find a subscriber or group of subscribers:

Step 1 In the Find field (see 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 non-contiguous subscribers

To select a range of subscribers:

Select the first subscriber in the range, then hold down the **<Shift>** key on the keyboard and click on the last subscriber in the range.

All subscribers in the range are selected.

This function can be combined with the search function; search to display specific subscribers, then select the entire range.

To select a number of non-contiguous subscribers:

Hold down the **<Ctrl>** key on the keyboard while selecting subscribers.


This function can be combined with selecting a range of subscribers; first select the range of subscribers, and then select additional subscribers, as required.

Adding Subscribers

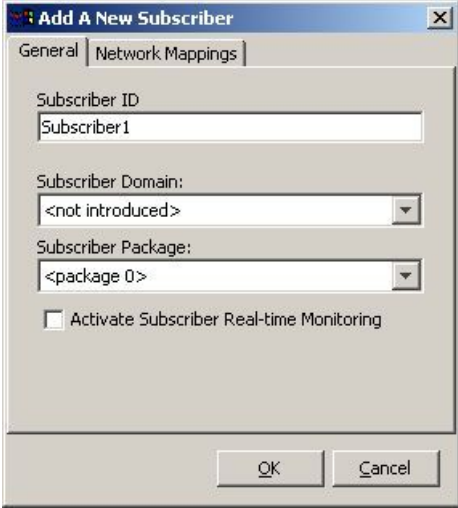
You can add additional individual subscribers to the SCMS-SM.

To add large number of subscribers, export their information from a Radius server (or similar) to a CSV file, and then import the CSV file (see *Working with Subscriber CSV Files* (on page 11-5)).

To add a subscriber:

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.

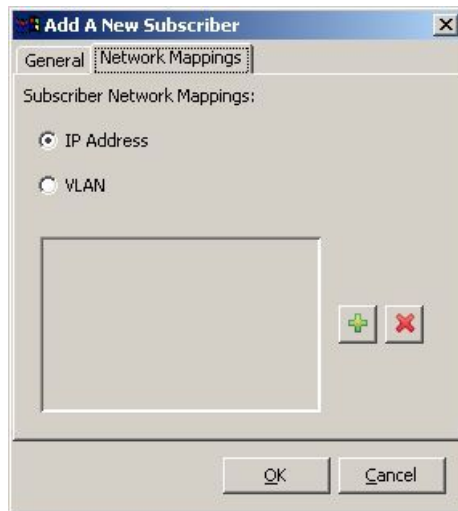
Step 4 From the Subscriber Package drop-down list, select a package to assign to this subscriber. The contents of the list depend on the selected subscriber domain.

Step 5 To activate subscriber real-time monitoring, check the **Activate Subscriber Real-time Monitoring** check box. This causes the SCE application to generate Subscriber Real-time Usage RDRs for this subscriber. For more information, see *Managing Real-Time Subscriber Usage RDRs* (on 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 of the Add a New Subscriber dialog box appears.



The system supports either IP addresses or VLAN tags as network identification for subscribers.

Step 7 Click 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 field appears in the subscriber network mappings list, displaying a default value.

Step 9 Edit the network mapping field.



Step 10 Repeat steps 8 and 9 as required.

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 Subscribers

You can edit parameters of specific subscribers one at a time, or edit a group of subscribers in one go.

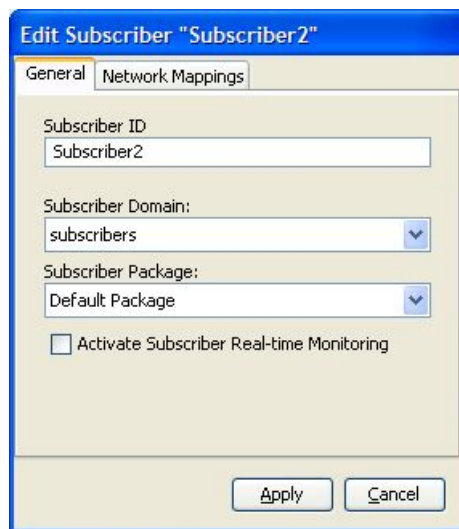
Editing Single Subscribers

To edit subscriber information:

Step 1 Find (see *Finding Subscribers* (on page 11-8)) and select a subscriber.

Step 2 In the SM toolbar, click  (**Edit Subscriber**).

The Edit Subscriber dialog box appears.



The screenshot shows a dialog box titled "Edit Subscriber 'Subscriber2'". It has two tabs: "General" (selected) and "Network Mappings". The "General" tab contains the following fields:

- Subscriber ID: A text box containing "Subscriber2".
- Subscriber Domain: A drop-down menu with "subscribers" selected.
- Subscriber Package: A drop-down menu with "Default Package" selected.
- Activate Subscriber Real-time Monitoring: An unchecked checkbox.

At the bottom of the dialog box are two buttons: "Apply" and "Cancel".

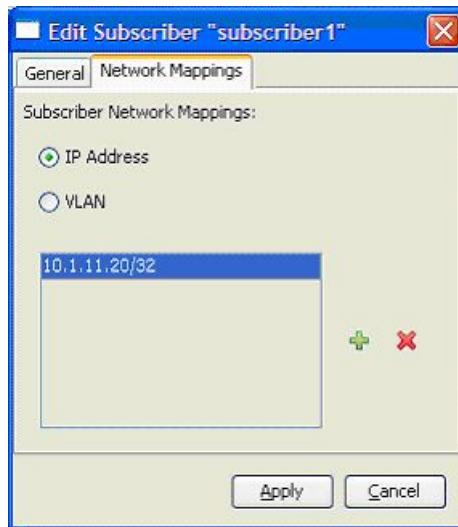
Step 3 Modify subscriber details as required:

- Subscriber ID—Edit the entry in the field.
- Subscriber Domain—From the drop-down list, select a subscriber domain.
- Subscriber Package—From the drop-down list, select a package to assign to this subscriber. The contents of the list depend on the selected subscriber domain.
- Activate Subscriber Real-time Monitoring—Check or uncheck the 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 of the Edit Subscriber dialog box appears.



Step 5 Modify subscriber network mappings as required:

- Click one of the **Subscriber Network Mappings** radio buttons:
 - **IP Address**
 - **VLAN**
- 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
- To delete a network mapping from the list:
 - Select an entry in the subscriber network mappings list and click **-** (**Remove**)

Step 6 Click **Apply**.

The Edit Subscriber dialog box closes.

The modified subscriber information is saved to the database; the modified information is displayed in the subscriber list displayed in the SM GUI tool.

Editing Multiple Subscribers

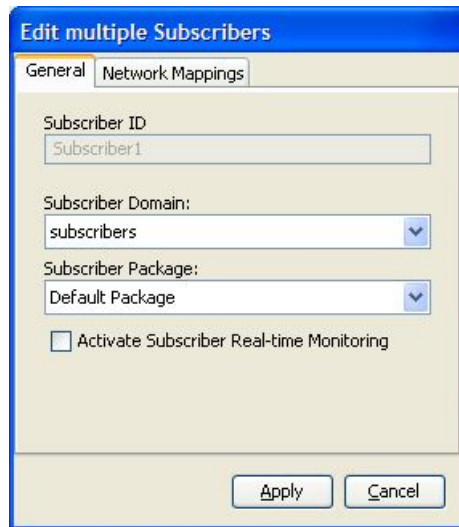
You can assign the same package or domain to many subscribers at one time.

To edit details for a group of subscribers:

Step 1 Select a group of subscribers to modify (see *Selecting Subscribers* (on page 11-8)).

Step 2 In the SM toolbar, click **Edit**.

The Edit Multiple Subscribers dialog box appears.



This differs from the regular Edit Subscriber dialog box in the following ways:

- The Subscriber ID field is dimmed; it displays the name of the last subscriber added to the group
- The Network Mappings tab is disabled

Step 3 Modify fields in the General tab as required:

- Subscriber Domain—From the drop-down list, select a subscriber domain.
- Subscriber Package—From the drop-down list, select a package to assign to this subscriber. The contents of the list depend on the selected subscriber domain.
- Activate Subscriber Real-time Monitoring—Check or uncheck the check box.

Step 4 Click **Apply**.

The Edit multiple Subscribers dialog box closes.


The modified subscriber information is saved to the database; the modified information is displayed in the subscriber list displayed in the SM GUI tool.

Deleting Subscribers

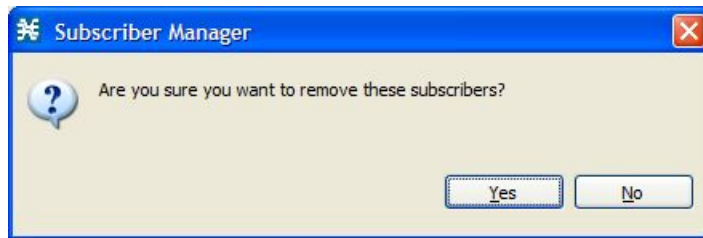
You can delete subscribers from the database.

To delete a subscriber from the database:

Step 1 Select a single subscriber or a group of subscribers (see *Selecting Subscribers* (on page 11-8)).

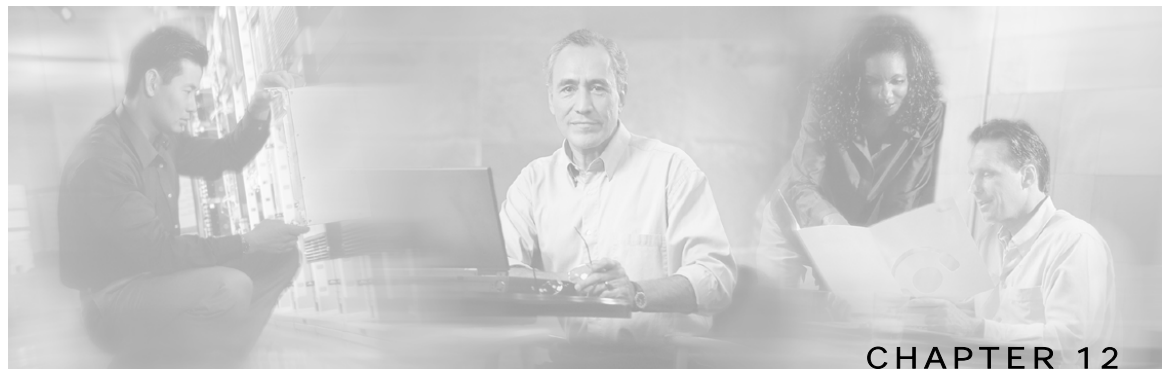
Step 2 In the SM toolbar, click  (**Remove Subscriber**).

The system asks for confirmation before removing the selected subscribers:



Step 3 Click **Yes** to confirm.

The selected subscribers are deleted from the database; they are removed from the subscriber list displayed in the SM GUI tool.



Using the Signature Editor

The Signature Editor tool allows you to create and modify Dynamic Signature Script (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 specific network protocols that are not yet supported by *SCA BB*.

This chapter contains the following sections:

- [Managing DSS Files](#) 12-1

Managing DSS Files

The DSS file components, and the creation and editing of DSS files are explained in the following sections.

- Installing new signatures to an active service configuration is described in *Installing Protocol Packs* (on page 4-8)
- Working with signatures in the Service Configuration Editor is described in *Managing Protocol Signatures: Dynamic Signatures* (on page 7-32)
- Using servconf, the Server Configuration Utility, to apply signatures is described in *The Cisco Service Control Application for Broadband Service Configuration Utility* (on page 13-1)

DSS File Components

The DSS file components are displayed in the Script tab 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.

The components are described in the following sections.

The DSS File

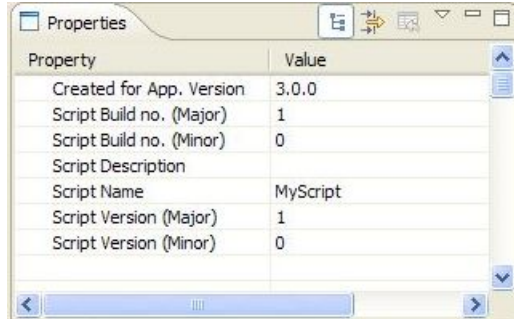
The DSS file name is the root node of the DSS file component tree.

When you select the root node, you can define the following properties for the DSS file:

- Created for Application Version—Select from a list of predefined values

- Script Build Number (Major)
- Script Build Number (Minor)
- Script Description—Enter the reason for creating this script and describe its contents
- Script Name—Enter a meaningful name for this script
- Script Version (Major)
- Script Version (Minor)

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.

The protocol list contains all the protocols that are being added, modified, or enhanced.

DSS Protocols

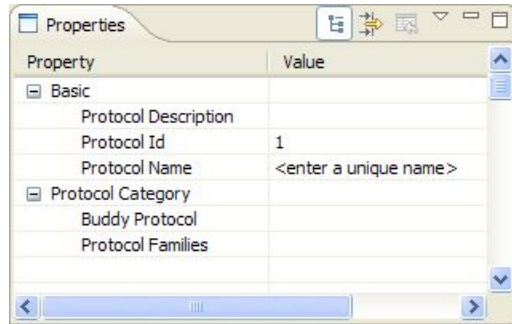
When you select a protocol node in the DSS file component tree, you can define the following properties of the protocol:

- Protocol Description
- Protocol ID—A unique value; the following section explains what value to enter in this field
- Protocol Name—A unique name; the following section explains what name to enter in this field
- Buddy Protocol—See *The Buddy Protocol* (on page [12-3](#))
- Protocol Families—Enter one or more of 'P2P', 'VOIP', and 'SIP', or leave blank

Protocol Family names are case sensitive

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 ID and Name

A DSS can include two types of protocols:

- A protocol that is not supported by *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 these two cases:

- The protocol is new to *SCA BB*—The name must not match any protocol name that *SCA BB* already supports. To see a list of all protocols that *SCA BB* already supports open the Protocol Settings dialog box in the Service Configuration Editor (see *Viewing Protocols* (on page 7-21)). Assign the protocol a unique ID in the range 5000 to 9998.
- Enhancing 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 *Viewing Protocols* (on page 7-21)).

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, while 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".

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 a different *quick inspection condition*. A quick inspection condition is a condition or set of conditions whose purpose is to make a preliminary screening of a flow. The quick inspection condition is tested against the first payload packet of the flows.

These signature types and their quick inspection conditions are described in the following sections.

String Match signatures and Payload Length signatures can contain deep inspection clauses. A signature (whose quick inspection condition is met) will accept a flow if the conditions of any of its deep inspection clauses are 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:

- Quick Inspection Condition:

- 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 does match 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.



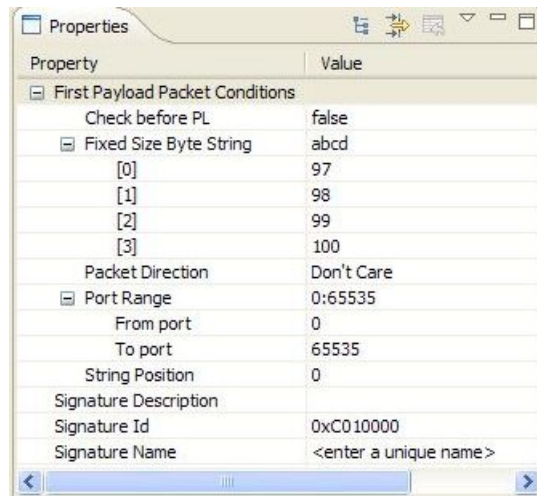
Caution

Check before PL should be set 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.

- 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
- 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 or 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)

- **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. If the string is to be matched with the beginning of the packet this value is 0. The value must be an integer divisible by four.
- **Signature Description:**
 - **Signature ID**—A value in the range 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
 - **Signature Name**—A unique name

The following screen capture shows the default values for the String Match signature properties.



Property	Value
First Payload Packet Conditions	
Check before PL	false
Fixed Size Byte String	
[0]	97
[1]	98
[2]	99
[3]	100
Packet Direction	Don't Care
Port Range	
From port	0
To port	65535
String Position	0
Signature Description	
Signature Id	0xC010000
Signature Name	<enter a unique name>

A flow that matches the quick inspection condition of a String Match Signature will then be compared against the deep inspection conditions of the signature (see *DSS Deep Inspection Conditions* (on page 12-8)).

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:

- **Quick Inspection Condition:**
 - **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 does match 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.

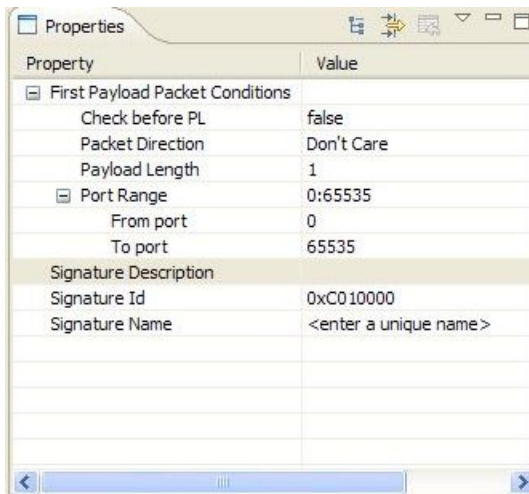


Caution

Check before PL should be set 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.

- **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 or 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)
- **Signature Description:**
 - **Signature ID**—A value in the range 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
 - **Signature Name**—A unique name

The following screen capture shows the default values for the Payload Length signature properties.



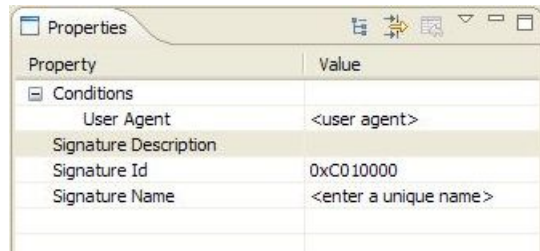
A flow that matches the quick inspection condition of a Payload Length Signature will then be compared against the deep inspection conditions of the signature (see *DSS Deep Inspection Conditions* (on page 12-8)).

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:

- **Quick Inspection Condition:**
 - **User Agent**—The value of the User Agent field in the HTTP header
- **Signature Description:**
 - **Signature ID**—A value in the range 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
 - **Signature Name**—A unique name

The following screen capture shows the default values for the HTTP User Agent signature properties.



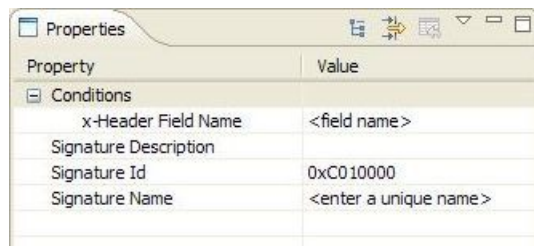
Property	Value
Conditions	
User Agent	<user agent>
Signature Description	
Signature Id	0xC010000
Signature Name	<enter a unique name>

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:

- Quick Inspection Condition:
 - x-Header Field Name—A name of a field in the x-Header of the HTTP header
- Signature Description:
 - Signature ID—A value in the range 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
 - Signature Name—A unique name

The following screen capture shows the default values for the DSS file properties.



Property	Value
Conditions	
x-Header Field Name	<field name>
Signature Description	
Signature Id	0xC010000
Signature Name	<enter a unique name>

DSS Deep Inspection Clauses

A deep inspection clause is a conjunctive clause of deep inspection conditions; a signature will accept a flow if all conditions within 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 has been accepted by the quick inspection condition, the clause containing the condition with the lowest Packet Number is tested first; 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 quick inspection condition screening of String Match signatures or Payload Length signatures.

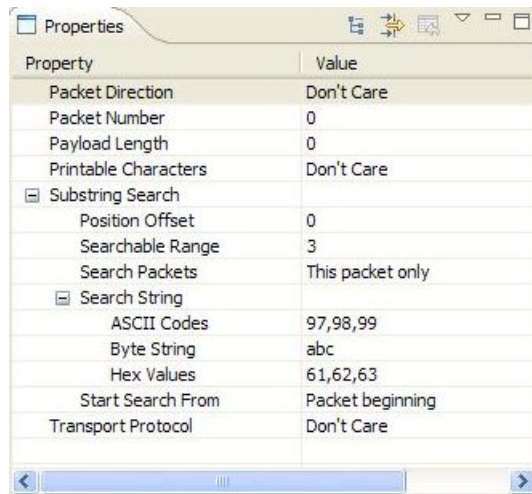
When you select a deep inspection condition node in the DSS file component tree, you can define the following properties of the deep inspection condition:

- **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 or 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 '0' 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, or 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
 - **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 or 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
 - **Start Search From**—This field can have one of two values: Packet beginning or Last match

Last match means that the search for this search string starts where the last search match ended. The last match can be from a previous substring search or from the last string-based Quick Inspection Condition.
- **Transport Protocol**—This field can have one of three values: TCP, UDP, or Don't Care (either TCP or UDP).

The following screen capture shows the default values for the deep inspection condition properties.



Property	Value
Packet Direction	Don't Care
Packet Number	0
Payload Length	0
Printable Characters	Don't Care
<input checked="" type="checkbox"/> Substring Search	
Position Offset	0
Searchable Range	3
Search Packets	This packet only
<input checked="" type="checkbox"/> Search String	
ASCII Codes	97,98,99
Byte String	abc
Hex Values	61,62,63
Start Search From	Packet beginning
Transport Protocol	Don't Care

The structure of deep inspection conditions is the same for String Match signatures and Payload Length signatures.


Creating DSS Files



Caution

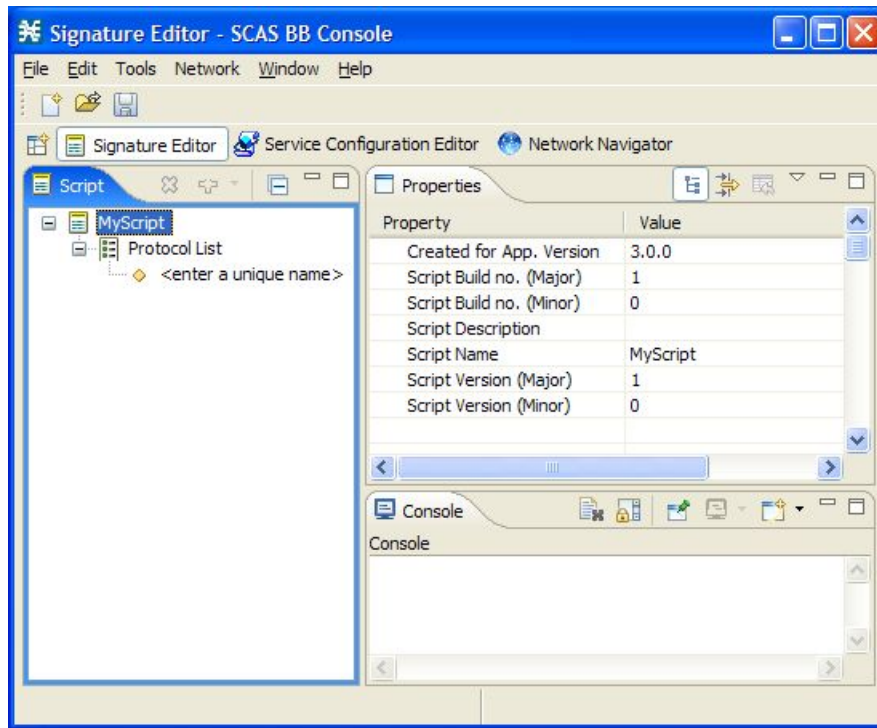
If you have a DSS file open in the Signature Editor, save it before you create a new DSS file; all unsaved changes will be lost.

To create a new DSS file:

- Step 1** From the toolbar, click on  (**Create a New DSS File**).

A DSS component tree containing a DSS file node, a protocol list node, and a protocol node, appears in the Script tab.

The default properties of the new DSS file are displayed in the Properties tab.



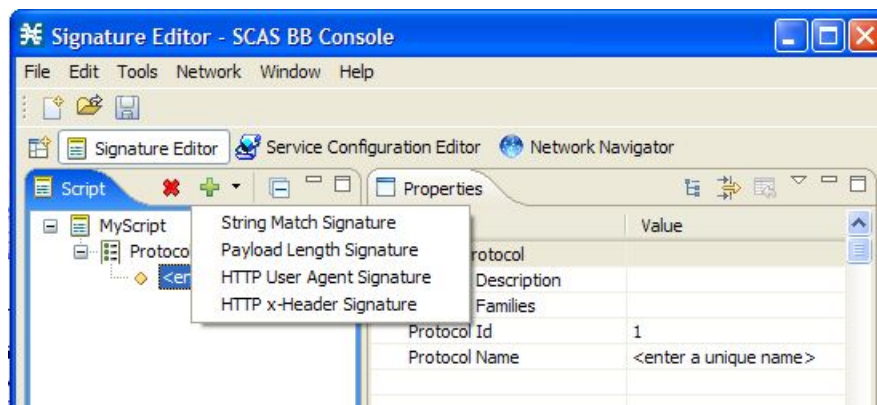
Step 2 Edit the DSS file properties (see *The DSS File* (on page 12-1) for an explanation of the properties).

Step 3 Click on the protocol node.

The protocol properties appear in the Properties tab.

Step 4 Edit the protocol properties (see *DSS Protocols* (on page 12-2) for an explanation of the properties).

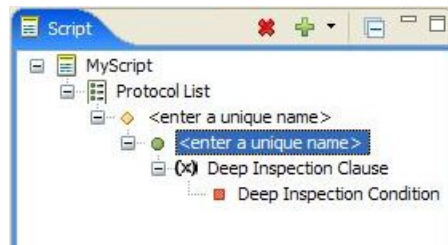
Step 5 Click on the drop-down arrow next to the **+** button.



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 on the signature node.

The signature properties appear in the Properties tab.

Step 8 Edit the signature properties (see *DSS Signatures* (on page 12-3) for an explanation of the properties).

Step 9 If you selected a String Match signature or a Payload Length signature:

a) Click on the deep inspection condition node.

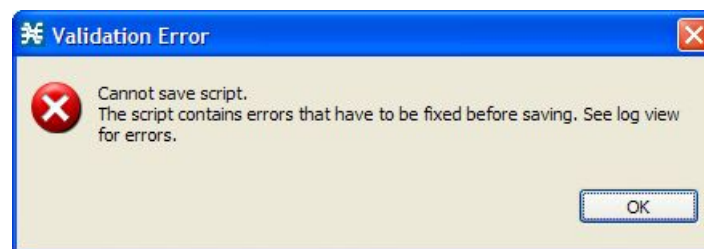
The deep inspection condition properties appear in the Properties tab.


b) Edit the deep inspection condition properties (see *DSS Deep Inspection Conditions* (on page 12-8) for an explanation of the properties).

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, then click  (**Save**) again.

A Save As dialog box appears.

Step 12 Browse to the folder where the new DSS file should be saved.

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.

Editing 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.

To edit an existing DSS file:

Step 1 From the toolbar, click on  (**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 tab.

The DSS file node is selected, and the properties of the DSS file are displayed in the Properties tab.

Step 4 Add, edit, or delete DSS file components as required. (See the subsections of *DSS File Components* (on page 12-1) for an explanation of the properties of the different components.)

Step 5 Save the modified DSS file:

- To overwrite the current DSS file with the changes you have made:

From the toolbar, click on  (**Save**).

The changes to the DSS file are saved.

- To save the modified DSS file with a new name:

a) From the **File** menu, choose **Save As**.

A Save As dialog box appears.

b) Browse to the folder where the new DSS file should be saved.

c) In the File name field, enter an appropriate name for the DSS file.

d) Click **Save**.

The Save As dialog box closes.

The modified DSS file is saved with the new name.

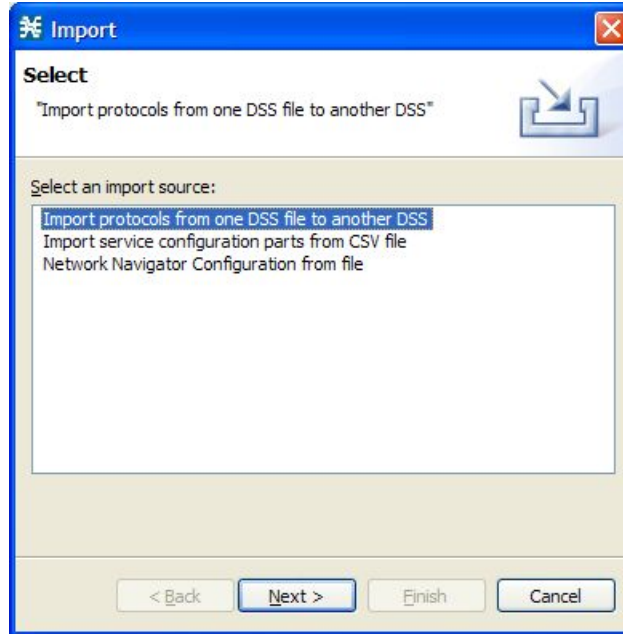
Importing Signatures

You can import DSS files into the file you are currently editing.

To import a DSS file:

Step 1 From the **File** menu, choose **Import**.

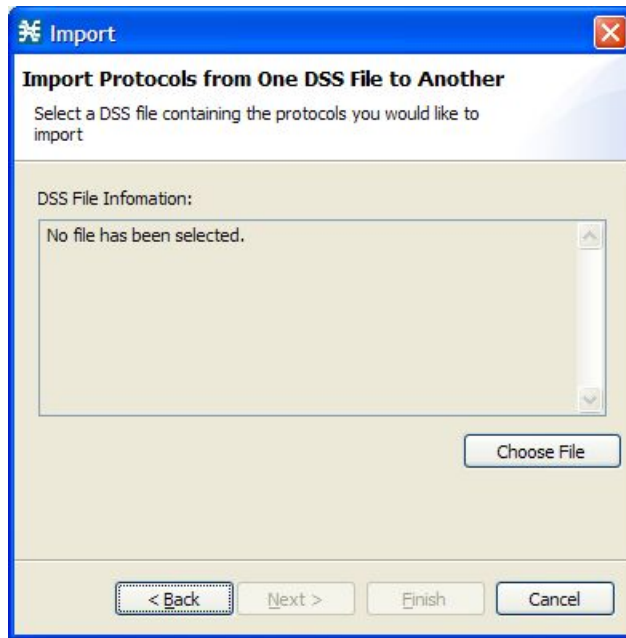
The Import dialog box appears.



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 appears.



Step 4 Click **Choose File**.

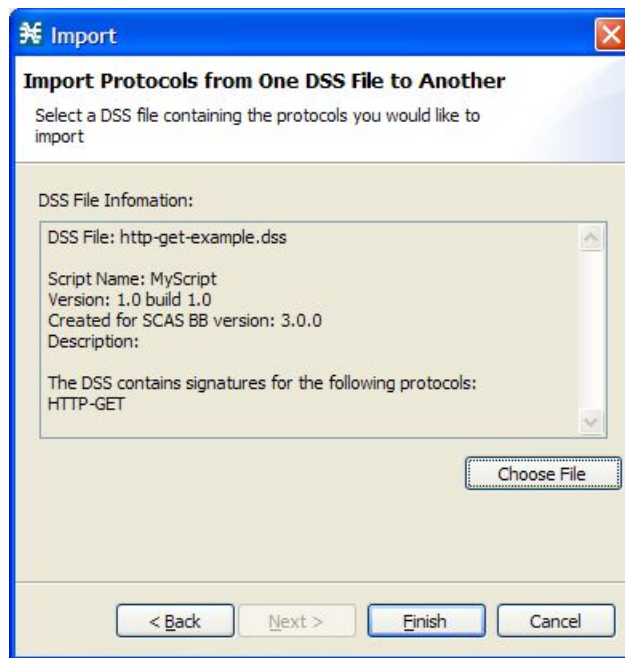
An Open dialog box appears.

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.



Note Importing signatures may create protocol name or protocol ID duplication.

The Signature Editor Console

The Signature Editor writes log and error messages to the Signature Editor Console (in the Console tab), when appropriate.



Additional Management Tools and Interfaces

This chapter contains the following sections:

- [The Cisco Service Control Application for Broadband Service Configuration Utility](#) 13-1
- [The SCA BB Signature Configuration Utility](#) 13-4
- [Attack Filtering and Subscriber Notification](#) 13-5
- [SNMP, MIB, and Traps: Overview](#) 13-11
- [Managing Subscribers via Other System Components](#) 13-12

The Cisco Service Control Application for Broadband 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 SCE platforms.

The service configuration utility can be used in Windows, Solaris, and Linux environments.

For installation instructions, see *Installing the SCA BB Configuration Utilities* (on page 4-8).

Using the SCA BB Service Configuration Utility

The command-line syntax of the *SCA BB* Service Configuration Utility is:

```
servconf [CONNECTION] <OPERATION> [FILE] [REFER-SE]
```

The following tables list the `servconf` operations and options.

Table 13-1 servconf Operations

Operation	Abbreviation (if applicable)	Description
<code>--apply</code>	<code>-a</code>	Copies the specified service configuration file to the specified SCE platforms and activates it

Operation	Abbreviation (if applicable)	Description
<code>--retrieve</code>	<code>-r</code>	Retrieves the current service configuration
<code>--update-dc</code>	<code>-u</code>	Updates a Cisco Service Control Management Suite (SCMS) Collection Manager (CM) with the service configuration values
<code>--status</code>		Shows the service configuration status on the SCE platform
<code>--update-signature</code>		Updates the SCE platform with a new protocol pack
<code>--update-signature-pqi</code>		Updates the SCE platform with a new SPQI protocol pack
<code>--signature-info</code>	<code>-i</code>	Shows information about the Dynamic Signature Script (DSS) file
<code>--help</code>		Displays help, then exits
<code>--version</code>		Displays the program version number, then exits

Table 13-2 servconf File Options

File Option	Abbreviation	Description
<code>--file=filename</code>	<code>-f</code>	Specifies service configuration file or DSS file
<code>--backup-directory=directory</code>	<code>-b</code>	Specifies the directory where the retrieved PQB file is to be saved prior to applying a new protocol pack

Table 13-3 servconf Connection Options

File Option	Abbreviation	Description
<code>--se=address</code>	<code>-S</code>	Specifies the 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.
<code>--dc=address</code>	<code>-D</code>	Specifies the address of the destination SCMS-CM platform (required only for the <code>--update-dc</code> operation).
<code>--password=password</code>	<code>-P</code>	Specifies the password for connecting to the SCE platform.

Table 13-4 servconf Reference SCE Option

File Option	Description
<code>--refer-se=address</code>	Specifies the address of the SCE platform to which the service configuration values refer (required only for <code>--update-dc</code> operation)

Table 13-5 servconf Apply Options

File Option	Description
<code>--no-dc</code>	An optional flag that specifies that the <code>--apply</code> operation should not automatically update the SCMS-CM with service configuration values.
<code>--no-default-signature</code>	Applies the service configuration without adding the Default DSS to it.
<code>--force-default-signature</code>	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
<code>--force-signature</code>	Forces the 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.

SCA BB Service Configuration Utility Examples

EXAMPLE 1

The following example shows how 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" --password ***** --apply --file config.pqb
```

EXAMPLE 2

The following example shows how 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 -P ***** --retrieve --file my_files/config.pqb
```

EXAMPLE 3

The following example shows how 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 -P ***** --update-dc --refer-se 63.111.106.7 --file config.pqb
```

EXAMPLE 4

The following example shows how 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" -p *****
```

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 be used in Windows, Solaris, and Linux environments.

For installation instructions, see *Installing the SCA BB Configuration Utilities* (on page 4-8).

Using the SCA BB Signature Configuration Utility

The command-line syntax of the *SCA BB* Signature Configuration Utility is:

```
sigconf <OPERATION> [FILE]
```

The following tables list the `sigconf` operations and options.

Table 13-7 sigconf Operations

Operation	Abbreviation	Description
<code>--set-default-dynamic-signature</code>	<code>-d</code>	Installs the Default DSS on this workstation
<code>--remove-default-dynamic-signature</code>		Uninstalls the Default DSS from this workstation
<code>--get-default-dynamic-signature</code>		Fetches the Default DSS installed on this workstation
<code>--help</code>		Displays help, then exits

Table 13-8 sigconf File Option

File Option	Abbreviation	Description
<code>--file=filename</code>	<code>-f</code>	Specifies DSS file

SCA BB Signature Configuration Utility Examples

EXAMPLE 1

The following example shows how to install the file `new_signature.dss` as the default DSS:

```
sigconf --set-default-dynamic-signature --file new_signature.dss
```

EXAMPLE 2

The following example shows how to retrieve the installed default DSS file, and save it as `default_backup.dss`:

```
sigconf --get-default-dynamic-signature --file default_backup.dss
```

Attack Filtering and Subscriber Notification

Attack filtering is a feature of the SCE platform whose aim is to detect attacks that occur in the traffic flowing through the SCE platform, to report such attacks via management channels, and to handle the attacks by blocking them, if configured to do so. In addition, with *SCA BB* running on the SCE platform, a subscriber whose IP address is associated with an attack can be notified about the attack on-line by the SCE platform.

This section describes how to enable subscriber notifications as part of the attack filtering and handling settings. See the *Attack Filtering* chapter in the *Cisco Service Control Engine Software Configuration Guide* for a complete description of attack detection and handling.

You can also enable the generation of Attack Signaling Raw Data Records (RDRs) for selected packages (see *Managing Real-Time Signaling RDRs* (on page 8-14)).

Subscriber Notification on Network Attack

Subscriber notification is a feature that can be used to notify a subscriber in real-time about current attacks involving IP addresses mapped to that subscriber. *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. (For other uses of subscriber notifications, see *Managing Subscriber Notifications* (on page 10-9).)

When an attack is identified, if the IP address is detected on the subscriber side and is mapped to a subscriber, *SCA BB* stores information about the attack. This allows *SCA BB* to notify the subscriber about the attack on-line, by redirecting subsequent HTTP requests of this subscriber to a server that will notify them of the attack.

In addition, when blocking TCP traffic, the system can be configured to not block specified ports to make this redirection possible. A list of up to three port numbers can be configured to be unblockable.

Destination URL

Once an attack is identified, HTTP flows of the subscriber are redirect to a configurable destination URL. For example, all HTTP flows can be redirected to a URL such as "http://www.some-isp.net/warning.html", which will warn the subscriber about the attack.

Optionally, a tail with a description of the attack can be added to the destination URL. This tail can be used by the destination server to create a more specific warning. The tail is added as the "query-part" of the URL, and 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 the following table:

Table 13-9 Description Tail Fields

Field	Indicates
side	<ul style="list-style-type: none"> • s=subscriber • n=network

dir	<ul style="list-style-type: none"> • s=source • d=destination
protocol	<ul style="list-style-type: none"> • TCP • UDP • ICMP • OTHER
open-flows	Number of open flows
suspected flows	Number of attack-suspected flows
open-flows-threshold	Threshold for open flows
suspected-flows-threshold	Threshold for attack-suspected flows
action	<ul style="list-style-type: none"> • B=block • R=report
handled-flows	<p>Number of handled flows since the attack began</p> <p>(Non-zero only during and at the end of an attack)</p>

Thus, a URL with a description tail may, for example, look like this:

```
http://www.some-isp.net/warning?ip=80.178.113.222&side=s&dir=s&prot=TCP&no=34&nd=4&to=34&td=10&ac=B&nh=100
```

Dismissal URL

All HTTP flows are redirected until the notification is dismissed. The notification is dismissed when the subscriber accesses the dismissal URL. By default, the destination URL is also the dismissal URL, so a notification is dismissed once the first redirection takes place. However, it is possible to define a different dismissal URL, so that the subscriber must acknowledge the notification.

The dismissal URL includes the URL hostname and the URL path, separated by a colon, in the following format:

```
[ * ]<hostname> : <path> [ * ]
```



Note

The path element must always start with '/'.

The hostname may optionally be preceded by a wildcard (*), to match all hostname with the same suffix. Similarly, the path may be followed by a wildcard, to match all paths with a common prefix. This makes it possible to define a range of URLs for dismissal.

For example, the entry:

```
*.some-isp.net:/redirect/*
```

matches all these URLs:

```
www.some-isp.net/redirect/index.html
```

```
support.some-isp.net/redirect/info/warning.asp
```

```
v4.windowupdate.some-isp.net/redirect/acknowledge.aspx?ie=UTF-8
```

Allowed-URL List

When a notification is active, 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, by adding them to the allowed-URL list. This can be useful, for example, to give subscribers access to additional support information.

Each entry in the allowed URL list has the same format as the dismissal URL, described in the preceding section.

Configuring Attack Subscriber Notifications

Subscriber notification is configured, as are other attack filtering settings, using the SCE CLI.

The formats of <Destination URL>, <Dismissal URL>, and <Allowed URL> are described in the preceding sections.



Note Attack Filtering Subscriber Notification settings are not part of the service configuration PQB file.

To enable subscriber notification redirection and configure a destination URL:

Step 1 At the SCE# prompt type:

```
configure and press Enter
```

The SCE(config)# prompt appears.

Step 2 Type:

```
interface linecard 0 and press Enter
```

The SCE(config if)# prompt appears.

Step 3 Type:

```
attack-filter subscriber-notification redirect destination-URL  
<Destination URL>
```

The destination URL must be complete, including the `http://` prefix, hostname and path. For example, `http://www.some-isp.net/redirect.html` is a valid destination URL, while `www.some-isp.net` is not.

To disable subscriber notification redirection:

Step 1 At the SCE# prompt type:
configure and press **Enter**

The SCE(config)# prompt appears.

Step 2 Type:
interface linecard 0 and press **Enter**

The SCE(config if)# prompt appears.

Step 3 Type:
no attack-filter subscriber-notification redirect destination-URL



Note This command also dismisses all currently active notifications.

To enable the attack description tail:

Step 1 At the SCE# prompt type:
configure and press **Enter**

The SCE(config)# prompt appears.

Step 2 Type:
interface linecard 0 and press **Enter**

The SCE(config if)# prompt appears.

Step 3 Type:
attack-filter subscriber-notification redirect tail

To disable the attack description tail:

Step 1 At the SCE# prompt type:

configure and press **Enter**

The SCE(config)# prompt appears.

Step 2 Type:

interface linecard 0 and press **Enter**

The SCE(config if)# prompt appears.

Step 3 Type:

no attack-filter subscriber-notification redirect tail

To set a dismissal URL:

Step 1 At the SCE# prompt type:

configure and press **Enter**

The SCE(config)# prompt appears.

Step 2 Type:

interface linecard 0 and press **Enter**

The SCE(config if)# prompt appears.

Step 3 Type:

**attack-filter subscriber-notification redirect dismissal-URL
<Dismissal URL>**

To delete the dismissal URL:

Step 1 At the SCE# prompt type:

configure and press **Enter**

The SCE(config)# prompt appears.

Step 2 Type:

```
interface linecard 0 and press Enter
```

The SCE(config if)# prompt appears.

Step 3 Type:

```
no attack-filter subscriber-notification redirect dismissal-URL
```

The destination URL is used for dismissal instead of the previously configured dismissal URL.

To add a URL to the allowed-URL list:

Step 1 At the SCE# prompt type:

```
configure and press Enter
```

The SCE(config)# prompt appears.

Step 2 Type:

```
interface linecard 0 and press Enter
```

The SCE(config if)# prompt appears.

Step 3 Type:

```
attack-filter subscriber-notification redirect allowed-host  
<Allowed URL>
```

To clear the allowed-URL list:

Step 1 At the SCE# prompt type:

```
configure and press Enter
```

The SCE(config)# prompt appears.

Step 2 Type:

```
interface linecard 0 and press Enter
```

The SCE(config if)# prompt appears.

Step 3 Type:

```
no attack-filter subscriber-notification redirect allowed-host
```

To monitor the attack filter subscriber notification settings:

Step 1 At the SCE# prompt type:

```
show interface LineCard 0 attack-filter subscriber-notification
redirect
```

This is an example of the output of this CLI command:

```
Attack-Filter Subscriber-Notification Redirection Settings:
Destination URL: http://www.my-isp.net/warning
Tail is used.

Dismissal URL: www.my-isp.net:/acknowledge*

Allowed Hosts:
*.my-isp.net:/softwareupdate/*
*.my-isp.net:/support/*
```

SNMP, MIB, and Traps: Overview

Cisco provides complete network FCAPS (Fault, Configuration, Accounting, Performance, Security) Management.

Two interfaces are provided for network management:

- **Command-Line Interface (CLI)**

The CLI is accessible through the Console port or through a Telnet connection.

CLI is used for configuration and security functions.

- **SNMP**

SNMP provides fault management via SNMP traps, as well as performance monitoring functionality.

SNMP

SNMP (Simple Network Management Protocol) 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 a Simple Network Management Protocol (SNMP) agent that supports the RFC 1213 standard (MIB-II) and the Cisco enterprise MIBs.

Configuring the SNMP agent parameters and enabling the SNMP interface is described in the *Cisco Service Control Engine 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 as defined in RFC 1213, Management Information Base for Network Management of TCP/IP-based Internets
- Cisco enterprise MIB, which is described by a number of MIB files.

The SCE proprietary MIB enables external management systems to retrieve general information regarding the SCE platform operating status and resources utilization, extract real time measurements of bandwidth utilization and network statistics, and receive notifications of critical events and alarms.

That part of the SCE proprietary MIB that provides configuration and runtime status for *SCA BB* is documented in the *Cisco Service Control Application for Broadband Reference Guide*.

Other parts of the SCE proprietary MIB are documented in *Cisco Service Control Engine Software Configuration Guide*. These guides also explain the order in which the MIB must be loaded.

Traps

Traps are unsolicited messages that are 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 RFC1157 and using the conventions defined in RFC1215
- Proprietary SCE enterprise traps—As defined in the SCE proprietary MIB

For a description of the SNMP traps and an explanation of how to configure the SNMP trap managers, see the *Cisco Service Control Engine Software Configuration Guide*.

Managing Subscribers via Other System Components

Other components of the Cisco Service Control solution offer alternatives for subscriber management. In addition to working directly via the Cisco Service Control Management Suite (SCMS) Subscriber Manager (SM), as opposed to accessing the SM from the SCAS BB Console, the SCE platform itself has a wide range of subscriber-related functions.

This section gives an overview of these options, with emphasis on the *SCA BB*-specific subscriber management options. For in-depth explanations, see the appropriate Service Control documentation.

Anonymous-Subscriber Mode

An anonymous subscriber is one with an internally generated 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. (See *Subscribers and Subscriber Modes* (on page 2-3).)

An anonymous group is a specified IP range, possibly assigned a subscriber template. When an anonymous group is configured, the SCE platform generates anonymous subscribers for that group when it detects traffic with an IP address that is in the specified IP range. If a subscriber template has been assigned to the group, the anonymous subscribers generated have properties as defined by that template. If no subscriber template has been 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). CLI commands can be entered via a Telnet session. For more information, see the *Cisco Service Control Engine 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:



Note

The following CLI commands are line interface configuration commands. You must enter line interface configuration mode and see the SCE(config if)# prompt displayed.

- `subscriber anonymous-group import csv-file`
- `subscriber anonymous-group export csv-file`
- `subscriber template import csv-file`
- `subscriber template export csv-file`

Use the following commands to remove anonymous groups or subscriber templates from the system.



Note

The following CLI commands are line interface configuration commands. You must enter line interface configuration mode and see the SCE(config if)# prompt displayed.

- `no subscriber anonymous-group [all] [name "groupname"]`
- `clear subscriber anonymous`
- `default subscriber template all`

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—See *Using the Subscriber Manager GUI Tool* (on page 11-1)
- SCE platform CLI—As described in this section
- SM Command-Line Utilities (CLU)—As described in this section

SCE Platform Subscriber CLI

Use the following commands to import subscriber data from CSV files and to export subscriber data to these files:



Note

The following CLI commands are line interface configuration commands. You must enter line interface configuration mode and see the SCE(config if)# prompt displayed.

```
subscriber import csv-file
```

- `subscriber export csv-file`

Use the following command to remove subscribers from the system.



Note

The following CLI commands are line interface configuration commands. You must enter line interface configuration mode and see the SCE(config if)# prompt displayed.

- `no subscriber [all] [name "subscriber-name"]`

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`

SM CLU

Use the **p3subs** SM utility to manage subscribers. You can add or remove subscribers. You can also manage subscriber properties and mappings with this utility.

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

To manage subscribers:

At the Solaris shell prompt, enter a command having the following general format:

```
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 13-10 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 is to be monitored.



Caution

Generating and collecting Real-Time Subscriber Usage RDRs for many subscribers can cause performance penalties; enable Real-Time Subscriber Usage RDR generation only for those subscribers that must actually be monitored by the system.

The **monitor** subscriber property indicates whether the generation of Real-Time Subscriber Usage RDRs is enabled for the subscriber, as follows:

- Enabled—**monitor** = 1
- Disabled—**monitor** = 0 (default)

You can modify this property for selected subscribers using either the SM CLU or the SCE platform CLI.

Managing Subscriber Monitoring via the SM

You can enable/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*.

To enable subscriber monitoring for subscriber "Smith":

Run the following from the command line:

```
sm/server/bin/p3subs --set --subscriber Smith --property monitor=1
```

To disable subscriber monitoring for subscriber "Smith":

Run the following from the command line:

```
sm/server/bin/p3subs --set --subscriber Smith --property monitor=0
```

To enable subscriber monitoring for a group of 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 Run the following from the command line:

```
sm/server/bin/p3batch -f monitor.txt
```

You can check to see whether subscriber monitoring is enabled for a specific subscriber.

To see whether subscriber monitoring is enabled for subscriber "Smith":

Run the following from the command line:

```
sm/server/bin/p3subs --show-property --subscriber Smith --property
monitor
```

Managing Subscriber Monitoring via the SCE Platform

You can also enable/disable the generation of the real-time subscriber usage RDRs using the SCE platform. For more information, see the *Cisco Service Control Engine CLI Command Reference*.

(The prompt is included in these examples to illustrate how it changes. You must see the **SCE(config if)#** prompt to invoke the actual subscriber command.)

To enable subscriber monitoring for subscriber "Smith":

Run the following from the command line:

```
SCE# configure
SCE(config)# interface LineCard 0
SCE(config if)# subscriber name Smith property monitor value 1
```

To disable subscriber monitoring for subscriber "Smith":

Run the following from the command line:

```
SCE# configure
SCE(config)#interface LineCard 0
SCE(config if)# subscriber name Smith property monitor value 0
```

To enable subscriber monitoring for a group of 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 monitor value 1
```

Managing Subscribers via Other System Components

```
subscriber name George property monitor value 1
subscriber name Elaine property monitor value 1
subscriber name Kramer property monitor value 1
subscriber name Newman property monitor value 1
```

Step 2 Run the following from the command line:

```
SCE# script run monitor.txt
```

You can check to see whether subscriber monitoring is enabled for a specific subscriber.

To see whether subscriber monitoring is enabled for subscriber "Smith":

Run the following from the command line:

```
SCE# 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 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 *Cisco Service Control Application for Broadband Reference Guide*.

To import CSV files:

Step 1 At the Solaris shell prompt, enter a command having the following general format:

```
p3subsdB --import <filename>
```

To export CSV files:

Step 1 At the Solaris shell prompt, enter a command having the following general format:

```
p3subsdb --export <filename>
```

EXAMPLE:

The following example shows how to export subscribers with filtering options to a specified CSV file.

```
p3subsdb --export --prefix=a --output=silverSubscriberFile.csv
```




Glossary of Terms

A

Anonymous subscriber mode

A mode in which entities defined as IP addresses or VLANs are treated as subscribers. The correlation to actual subscriber IDs is not performed by the system, but can be performed externally by the collection system. Anonymous subscriber mode does not require an SCMS-SM.

B

Bump-in-the-wire topology

See Inline topology

BW Controllers

See Subscriber BW Controllers

C

CLI

One of the management interfaces to the SCE platform. It is accessed through a Telnet session or directly via the console port on the front panel of the SCE platform.

CM

A software application running on a Solaris or Linux platform that is responsible for receiving RDRs from the SCE platform and processing them.

Command-Line Interface

See CLI.

D

Downstream traffic

Traffic entering the SCE platform from the network side (that is, toward the subscribers).

Dynamic Signature

A dynamic signature is a signature that can be loaded to a running application; once loaded the application can identify the protocol associated with this signature.

Dynamic subscriber-aware mode

A mode in which the actual subscriber ID is associated with an IP address when the subscriber logs onto the network and is assigned an IP address. To operate in this mode, the system must be integrated with the OSS system that assigns IP addresses to subscribers (typically based on Radius or DHCP).

E**External Quota Management**

Provisioning of per-service quotas for individual subscribers by an external system, such as a pre-paid server or a policy-controller.

In External Quota Provisioning, usage counters are not automatically reset at the end of an aggregation period, nor is a specific quota limit provided uniformly to all subscribers as part of the package Parameters. Rather the quotas are provisioned individually via the external Quota Management system.

External Quota Provisioning

See External Quota Management.

F**Filter Rules**

The part of the service configuration that instructs the SCE platform to ignore some types of transactions based on Layer 3 and Layer 4 properties, and transmit them unchanged, bypassing the Cisco Service Control solution service.

Flow

All packets traveling in both directions on a single application layer connection (such as a TCP or UDP connection). A flow is identified by the tuple information: <Source IP, Destination IP, Source Port, Destination Port, IP Protocol>. (Note that if the IP protocol is neither TCP nor UDP, the port number is defined as '0'.)

In this guide, the term 'flow' represents bidirectional flows (packets from both the client and server of each connection). When referencing a unidirectional flow, this is explicitly mentioned.

Flow bundle

A group of one or more flows comprising the set of application-layer connections (such as a TCP or UDP connection) used in a single, logical application session. The semantics of flow-bundles are application dependant, and relate to the way each application spawns and negotiates additional flows as part of a single session. A few common examples are:

- An SIP (VoIP) flow bundle comprises the signaling flow as well as all the RTP/UDP flows containing the actual media data (voice)
- An RTSP (Streaming) flow bundle comprises the signaling flow as well as the RTP/UDP flows containing the audio and video transmissions
- AN FTP (file transfer) flow bundle comprises the control flow (used to login to an FTP server) and the actual file-transfer flows

In each of these cases, the SCE platform tracks the application communication to identify new connections created and bundle them into a single context. This is important for classification and accounting purposes, as otherwise these spawned flows would be unclassifiable.

G**Global Controllers**

Global controllers are used to control the total bandwidth percentage for a selected protocol or package for all subscribers.

See also Subscriber BW Controllers.

I**Inline connection mode**

The SCE platform physically resides on the data link between the subscriber side and the network side, and can both receive and transmit traffic.

L**List**

An IP address range or list of web addresses used to define a service.

N**Network-initiated transactions**

Transactions that are initiated by a host, on the network side, toward a subscriber.

O**Online subscriber**

A subscriber that is currently online. At any particular time, a number of online subscribers will be idle.

P**Package**

A collection of business policy rules, defining access levels to various services, charging parameters, and traffic control actions to be taken upon predefined events. Subscribers are assigned packages (plans) that determine how their network transactions are controlled and charged.

PQI (Cisco Installation) File

An application package file that is installed on the network SCE platforms and the Cisco Service Control Management Suite Collection Managers.

Q**Quota**

A (subscriber's) limit for a specific metric, such as bandwidth or volume.

Quota buckets

When the external quota management mode is selected, subscriber usage of a service is consumed from a predefined subscriber quota bucket. Each subscriber has four subscriber quota buckets. When a quota bucket is depleted, services that try to consume from that bucket are *breached*.

A quota manager that is external to the Service Control system replenishes quota buckets.

R**Raw Data Record**

See RDR.

RDR

A data record produced by the SCE platform that reports on events in the traffic. RDRs produced by the SCE platform are sent to the Cisco Service Control Management Suite Collection Manager and then stored in the Collection Manager database or forwarded to third-party systems. The RDR typically contains a quota (*see* Quota) request or reports service usage.

RDR Formatter

An internal component of the SCE platform that gathers the Raw Data Records (RDRs), formats them, and sends them to an external Cisco Service Control Management Suite Collection Manager.

Real-time subscriber usage monitoring

Subscribers are monitored in detail; usage information is frequently reported by the SCE platform to facilitate detailed reports.

Receive-only connection mode

The SCE platform does not reside physically on the data link, and therefore can only receive data, but does not transmit.

Rule

A service is assigned to a package by defining a rule for the package.

S**SCAS BB Console**

The user interface used for controlling the Cisco Service Control Application for Broadband; used to create, modify, and apply service configurations.

SCE platform

The SCE platform is a purpose-built service component and active enforcing system designed for enhancing service providers and backbone carrier networks. By identifying, classifying, and manipulating complex traffic flows at wire-speed, the SCE platform transforms simple transport networks into differentiated service delivery infrastructures for a wide variety of value-added IP applications, such as video streaming, VoIP, tiered services, and bilateral application-level SLAs.

The SCE platform seamlessly interfaces with existing network elements—including routers, switches, aggregators, subscriber management devices, and operational support systems—using industry standard interfaces and communications protocols.

The need to guarantee that packets passing through the network are processed at the rate they arrive makes it necessary to provide a custom-made hardware solution.

The SCE platform comes in three models—SCE 1000, SCE 2000 4xGBE, and SCE 2000 4/8xFE. There may be one or more SCE platforms in the provider network. Within the SCE platform, network transactions are analyzed and mapped to services that enforce the provider's policies.

In addition, the SCE platform implements the business logic of the system solution and performs transaction analysis in real-time. When so instructed, the SCE platform creates a Raw Data Record (RDR) to be sent for storage to the system's data repository, the Cisco Service Control Management Suite Collection Manager; or carries out other operations such as bandwidth or volume control.

Service

A value-added offering given by the service provider to its subscribers on top of its access network.

For each such commercial service the providers offer to their subscribers, a corresponding service is defined in the Cisco Service Control solution for classifying and identifying network transaction associated with the service, reporting on its usage, and controlling its traffic according to the business policy.

Service Configuration

The definition of services within the Cisco Service Control solution, the mapping of network transactions to their corresponding services, and the behavior of the SCE platform on them. The service configuration includes the definition of services, packages, Bandwidth Controllers, filter rules, and so on.

Service Control

The basic Cisco concept for enabling service providers to differentiate subscribers, detect real-time events, create premium services, actively control applications, and leverage their existing infrastructure.

Service Control Application

An SML program (*see* SML) that determines how the SCE platform operates.

Service Control Engine platform

See SCE platform.

Service Control Management Suite Collection Manager

See CM.

Service Control Management Suite Subscriber Manager

See SM.

Service Modeling Language

See SML.

Session (also called Transaction)

An instance of communication between network hosts. A precise definition of a session is application protocol (Layer 7) dependent.

Signature

A set of parameters that uniquely identify a protocol.

SLI (SML Loadable Image) File

A software package (part of a Cisco Service Control Application solution) that contains the SML application that is loaded onto an SCE platform. The SML application determines the behavior of the SCE platform. Different SCE platforms can have different SML applications, even when they are within the same POP. (Operators do not need to access the SLI file.)

SM

A middleware software component used in cases where dynamic binding of subscriber information and service configurations is required. The SM manages subscriber information and provisions it in real time to multiple SCE platforms. It can store subscriber service configurations information internally, and act as a state-full bridge between the AAA system (for example, RADIUS and DHCP) and the SCE platforms.

SML

The Cisco scripting language, which enables the definition of service-related events and the execution of actions on those events.

Static subscriber-aware mode

A mode in which a specific IP address is bound to each subscriber. This mode is useful when controlling enterprise customers, or when controlling subscribers in groups of predefined subnets (such as users of a specific CMTS/BRAS).

Subscriber

Service Provider client. There are two types of subscribers:

- Introduced Subscriber—A specific customer with an externally generated name. May be mapped to more than one IP address.
- Anonymous subscriber group—A subscriber with an internally generated name, generated automatically by the SCE platform according to an anonymous subscriber group specification. Always mapped to a single IP address. The actual identity of the subscriber is unknown to the system.

Subscriber aware mode

A mode in which actual subscribers are defined in the system, thus requiring no external correlation to subscriber IDs.

Subscriber Bandwidth Controllers

See BW Controllers.

Subscriber BW Controllers

Subscriber BW Controllers control traffic bandwidth for an individual subscriber.

See also Global Controllers.

Subscriber-initiated transactions

Transactions that are initiated by a host of a subscriber.

Subscriberless mode

A mode of the Cisco Service Control solution that requires no integration, so that the SCMS-SM is not required. This mode is not influenced by the number of subscribers or inbound IP addresses; the total number of subscribers using the monitored link is unlimited from the perspective of the SCE platform. It is the choice for sites where control and level analysis functions are required only at a global platform resolution.

T**Time-Based Rule**

An added-value rule that can be attached to either the Default Service rule or to any other rule. A time-based rule is applied for one of the user-defined time frames.

Traffic Discovery Reports

Statistics reports on network activity based on transaction usage records.

Transaction (also called Session)

An event in traffic that is recognized by a service control application. A transaction is distinguished according to its L3, L4, or L7 characteristics. Different protocols may have different transaction types.

U**Upstream traffic**

Traffic entering the SCE platform from the subscriber side.



Index

A

Accessing On-Line Help • 4-22
Activating and Deactivating Filter Rules • 10-9
Adding a Set of Redirection URLs • 10-17
Adding a Site to the Site Manager • 5-2
Adding Calendars • 9-27
Adding CM Devices to a Site • 5-4
Adding Database Devices to a Site • 5-5
Adding Devices to a Site • 5-3
Adding Dynamic Signatures to the Service Configuration • 7-34
Adding Filter Rules • 10-2
Adding Flavor Items • 7-53
Adding Flavors • 7-50
Adding Global Controllers • 9-34
Adding New Service Configurations • 6-2
Adding Packages • 9-4
Adding Protocol Elements • 7-27
Adding Protocols • 7-23
Adding Rules to a Package • 9-12
Adding SCE Devices to a Site • 5-3
Adding Service Elements • 7-10
Adding Services • 7-4
Adding SM Devices to a Site • 5-4
Adding Subscriber Notifications • 10-12
Adding Subscribers • 11-9
Adding Time-Based Rules to a Rule • 9-21
Adding VAS Table Parameters • 10-28
Adding VAS Traffic Forwarding Tables • 10-27
Adding Zone Items • 7-45
Adding Zones • 7-43
Additional Management Tools and Interfaces • 13-1
Allowed-URL List • 13-7
Anonymous subscriber mode • 1

Anonymous Subscriber Mode • 2-4
Anonymous-Subscriber Mode • 13-13
Applying a Service Configuration to SCE Platforms • 6-14
Applying and Retrieving Service Configurations • 6-13
Applying Service Configurations to SCE Devices • 5-9
Attack Filtering and Subscriber Notification • 13-5
Audience • x

B

Bandwidth Management • 3-11
Bump-in-the-wire topology • 1
BW Controllers • 1

C

Calendars • 3-11
Cisco Service Control Application for Broadband - Service Control for Broadband Service Providers • 1-2
Cisco.com • xiv
CLI • 1
Closing Service Configurations • 6-5
CM • 1
Collection • 1-5
Command-Line Interface • 1
Configuring Attack Subscriber Notifications • 13-7
Configuring the Redirection Parameters • 10-19
Configuring the Time Frames • 9-29
Connecting to an SCMS-SM • 11-2
Contacting TAC by Telephone • xv
Contacting TAC by Using the Cisco TAC Website • xiv
Controlling Traffic at Two Levels

Total and Internal • 3-13
 Conventions • xi
 Creating DSS Files • 12-9

D

Defining General Parameters for a Rule • 9-13
 Defining General Parameters for a Service • 7-5
 Defining General Parameters for Packages • 9-5
 Defining Global Controllers in a Dual Link System • 9-36
 Defining Hierarchical Settings for a Service • 7-5
 Defining Per-Flow Actions for a Rule • 9-14
 Defining Service Configurations in Practice • 3-17
 Deleting a Set of Redirection URLs • 10-20
 Deleting Calendars • 9-29
 Deleting Devices • 5-5
 Deleting Filter Rules • 10-8
 Deleting Flavor Items • 7-55
 Deleting Flavors • 7-51
 Deleting Global Controllers • 9-35
 Deleting Packages • 9-9
 Deleting Protocol Elements • 7-31
 Deleting Protocols • 7-25
 Deleting Rules • 9-19
 Deleting Service Elements • 7-19
 Deleting Services • 7-9
 Deleting Sites • 5-6
 Deleting Subscriber Notifications • 10-13
 Deleting Subscribers • 11-13
 Deleting Time-Based Rules • 9-25
 Deleting VAS Table Parameters • 10-30
 Deleting VAS Traffic Forwarding Tables • 10-27
 Deleting Zone Items • 7-47
 Deleting Zones • 7-44
 Destination URL • 13-5
 Disconnecting from an SCMS-SM • 11-5
 Dismissal URL • 13-6
 Displaying the Services Affected by a Rule • 9-20
 Distributing Protocol Packs • 4-10
 Document Revision History • ix
 Documentation CD-ROM • xiii
 Documentation Feedback • xiii
 Downstream traffic • 1

DSS Deep Inspection Clauses • 12-7
 DSS Deep Inspection Conditions • 12-8
 DSS File Components • 12-1
 DSS Files • 4-9
 DSS HTTP User Agent Signature • 12-6
 DSS HTTP x-Header Signature • 12-7
 DSS Payload Length Signature • 12-5
 DSS Protocol List • 12-2
 DSS Protocols • 12-2
 DSS Signatures • 12-3
 DSS String Match Signature • 12-4
 Duplicating Packages • 9-7
 Duplicating Service Elements • 7-15
 Dynamic Signature • 1
 Dynamic Signature Script Files • 7-32
 Dynamic Signatures • 3-5
 Dynamic subscriber-aware mode • 1

E

Editing Advanced Service Configuration Options • 10-21
 Editing Breach Handling Parameters for a Rule • 9-51
 Editing DSS Files • 12-12
 Editing Filter Rules • 10-7
 Editing Flavor Items • 7-54
 Editing Flavors • 7-51
 Editing Global Controllers • 9-35
 Editing Multiple Subscribers • 11-12
 Editing Package Quota Management Settings • 9-48
 Editing Package Subscriber BWCs • 9-40
 Editing Packages • 9-8
 Editing Protocol Elements • 7-30
 Editing Protocols • 7-24
 Editing Rules • 9-17
 Editing Service Elements • 7-16
 Editing Services • 7-8
 Editing Single Subscribers • 11-11
 Editing Subscriber Notifications • 10-13
 Editing Subscribers • 11-11
 Editing the Total Link Limits • 9-34
 Editing Time-Based Rules • 9-23
 Editing VAS Table Parameters • 10-29
 Editing Zone Items • 7-46
 Editing Zones • 7-44
 Enabling VAS Traffic Forwarding • 10-24
 Examples of Services • 3-3
 Exporting a Network Navigator Configuration • 5-25

Exporting Service Configuration Data • 6-5
 Exporting Subscriber Files • 11-6
 External Quota Management • 2
 External Quota Provisioning • 2

F

Filter Rules • 2
 Filtering the Protocols View • 7-22
 Filtering the Traffic Flows • 10-1
 Finding and Selecting Subscribers • 11-7
 Finding Subscribers • 11-8
 Firewall/NAT Requirements • 5-29
 Flavor Item • 3-6
 Flavor Types and Parameters • 7-48
 Flavors • 3-6
 Flow • 2
 Flow bundle • 2

G

Generating Tech Support Info Files for SCE
 Devices • 5-8
 Generating Tech Support Info Files for SM
 Devices • 5-16
 Getting Started • 4-1
 Global Bandwidth Control • 3-12
 Global Controllers • 2
 Global Controllers and VAS Flows • 10-23

I

Importing a Network Navigator
 Configuration • 5-27
 Importing Dynamic Signatures from the
 Default DSS File • 7-40
 Importing Service Configuration Data • 6-9
 Importing Signatures • 12-13
 Importing Subscriber Files • 11-5
 Initiating Side • 3-5
 Inline connection mode • 2
 Installing a Protocol Pack • 4-10
 Installing a SCA BB PQI File on an SCE
 Platform • 4-3
 Installing a SCA BB PQI File on an SM
 Device • 4-4
 Installing PQI Files on SCE Devices • 5-12
 Installing PQI Files on SM Devices • 5-17
 Installing Protocol Packs • 4-8
 Installing Protocol Packs on SCE Devices •
 5-9
 Installing SCA BB • 4-1

Installing SCA BB Application Components
 • 4-3
 Installing SCA BB Front Ends • 4-4
 Installing the Java Runtime Environment •
 4-8
 Installing the SCA BB Configuration
 Utilities • 4-8
 Installing the SCAS BB Console • 4-5
 Installing the SCE OS Software Package on
 SCE Devices • 5-13

L

Launching the SCAS BB Console • 4-14
 Link Bandwidth Limit • 3-11
 List • 3

M

Making Databases Accessible to the SCAS
 Reporter • 5-20
 Management and Collection • 1-4
 Managing Advanced Service Configuration
 Options • 10-21
 Managing Bandwidth • 9-31
 a Practical Example • 9-42
 Managing Calendars • 9-26
 Managing CM Devices • 5-19
 Managing CSV Files • 13-18
 Managing Database Devices • 5-20
 Managing Devices • 5-6
 Managing DSS Files • 12-1
 Managing Flavor Items • 7-52
 Managing Flavors • 7-48
 Managing Global Bandwidth • 9-31
 Managing Log RDRs • 8-10
 Managing Packages • 9-1
 Managing Protocol Elements • 7-26
 Managing Protocol Signatures
 Dynamic Signatures • 7-32
 Managing Protocols • 7-20
 Managing Quota RDRs • 8-6
 Managing Quotas • 9-48
 Managing RDR Settings • 8-1
 Managing Real-Time Signaling RDRs • 8-14
 Managing Real-Time Subscriber Usage
 RDRs • 8-12
 Managing Rules • 9-11
 Managing SCE Devices • 5-6
 Managing Service Configurations • 6-2
 Managing Service Elements • 7-10
 Managing Services • 7-1

- Managing Sites • 5-2
- Managing SM Devices • 5-15
- Managing Subscriber Bandwidth • 9-39
- Managing Subscriber Monitoring via the SCE Platform • 13-17
- Managing Subscriber Monitoring via the SM • 13-16
- Managing Subscriber Notifications • 10-9
- Managing Subscribers • 11-7
- Managing Subscribers on SM Devices • 5-17
- Managing Subscribers via Other System Components • 13-12
- Managing the System Settings • 10-14
- Managing Time-Based Rules • 9-21
- Managing Transaction RDRs • 8-4
- Managing Transaction Usage RDRs • 8-8
- Managing Usage Counters • 8-1
- Managing Usage RDRs • 8-2
- Managing VAS Table Parameters • 10-28
- Managing VAS Traffic Forwarding Settings • 10-23
- Managing Zone Items • 7-45
- Managing Zones • 7-42
- Mapping Flow Attributes to Services • 3-7
- Maximum Number of Flavor Items per Flavor Type • 7-52
- MIB • 13-12
- Moving Service Elements • 7-19

N

- Navigating in the SCAS BB Console • 4-16
- Network Management • 1-5
- Network Settings Requirements • 5-29
- Network-initiated transactions • 3

O

- Obtaining Documentation • xii
- Obtaining Technical Assistance • xiii
- Online subscriber • 3
- Opening Existing Service Configurations • 6-3
- Ordering Documentation • xiii
- Organization • x
- Other Traffic Processing Features • 3-16
- Overview • 1-1

P

- Package • 3
- Package Counters • 3-9

- Package Parameters • 9-1
- Packages • 3-10
- Password Management • 5-24
- PQI (Cisco Installation) File • 3
- Preface • ix
- Prerequisites • 4-2
- Protocol Elements • 3-4
- Protocol Packs • 4-9
- Protocols • 3-4

Q

- Quick Start with the SCAS BB Console • 4-23
- Quota • 3
- Quota buckets • 3
- Quota Management • 3-15

R

- Raw Data Record • 3
- RDR • 3
- RDR Formatter • 3
- RDRs • 3-9
- Real-time subscriber usage monitoring • 3
- Receive-only connection mode • 3
- Related Documentation • xi
- Removing Dynamic Signatures • 7-35
- Renaming the Time Frames • 9-28
- Renaming VAS Server Groups • 10-25
- Retrieving Service Configurations from SCE Devices • 5-11
- Retrieving the Online Status of CM Devices • 5-19
- Retrieving the Online Status of SCE Devices • 5-6
- Retrieving the Online Status of SM Devices • 5-15
- Rule • 4
- Rule Hierarchy • 9-12
- Rules • 3-11

S

- Saving the Current Service Configuration • 6-4
- SCA BB Service Configuration Utility Examples • 13-3
- SCA BB Signature Configuration Utility Examples • 13-4
- SCAS BB Console • 4
- SCE platform • 4
- SCE Platform Subscriber CLI • 13-14

- Selecting Quota Buckets for Rules • 9-49
 - Selecting Subscribers • 11-8
 - Selecting Subscribers for Real-Time Usage Monitoring • 13-15
 - Service • 5
 - Service Configuration • 2-5, 5
 - Service Configuration API • 2-6
 - Service Configuration Management • 1-5
 - Service Configurations • 3-16
 - Service Control • 5
 - Service Control Application • 5
 - Service Control Capabilities • 1-2
 - Service Control Engine platform • 5
 - Service Control Management Suite
 - Collection Manager • 5
 - Service Control Management Suite
 - Subscriber Manager • 5
 - Service Counters • 3-8
 - Service Elements • 3-3
 - Service Modeling Language • 5
 - Service Parameters • 7-2
 - Services • 3-2
 - Session (also called Transaction) • 5
 - Setting Advanced Package Options • 9-6
 - Setting Bandwidth Limits as the Sum of Two Links • 9-38
 - Setting BW Management Prioritization Mode • 9-46
 - Setting Global Controller Bandwidth Limits in a Dual Link System • 9-36
 - Setting Protocol ID and Name • 12-3
 - Setting Redirection Parameters • 10-16
 - Setting the Default DSS File • 7-37
 - Setting the Operational Mode of the System • 10-14
 - Setting the Service Index • 7-7
 - Signature • 5
 - Signatures • 3-5
 - SLI (SML Loadable Image) File • 5
 - SM • 5
 - SM CLU • 13-15
 - SML • 5
 - SNMP • 13-11
 - SNMP, MIB, and Traps
 - Overview • 13-11
 - SPQI Files • 4-9
 - Static Subscriber Mode • 2-4
 - Static subscriber-aware mode • 6
 - Subscriber • 6
 - Subscriber aware mode • 6
 - Subscriber Bandwidth Control • 3-12
 - Subscriber Bandwidth Controllers • 6
 - Subscriber BW Controllers • 6
 - Subscriber BWC Parameters • 9-39
 - Subscriber Information • 11-7
 - Subscriber Management • 1-5
 - Subscriber Modes
 - Summary • 2-5
 - Subscriber Notification • 3-15
 - Subscriber Notification on Network Attack • 13-5
 - Subscriber Notification Parameters • 10-9
 - Subscriber-Aware Mode • 13-14
 - Dynamic Subscribers • 2-4
 - Subscriber-initiated transactions • 6
 - Subscriberless mode • 6
 - Subscriberless Mode • 2-3
 - Subscribers and Subscriber Modes • 2-3
 - System Components • 2-1
 - System Overview • 2-1
 - System Requirements • 4-5
- T**
- Technical Assistance Center • xiv
 - The Buddy Protocol • 12-3
 - The Cisco Service Control Application for Broadband Service Configuration Utility • 13-1
 - The Cisco Service Control Concept • 1-1
 - The Default DSS File • 7-37
 - The Default Service Rule • 9-12
 - The DSS File • 12-1
 - The Network Navigator Tool • 4-17, 5-1
 - The Package Hierarchy • 3-9
 - The Reporter Tool • 4-21
 - The SCA BB Installation Package • 4-3
 - The SCA BB Service Configuration Utility • 2-6
 - The SCA BB Signature Configuration Utility • 13-4
 - The SCAS BB Console • 2-6
 - The SCE Platform • 1-3
 - The Service Configuration Editor Tool • 4-18, 6-1
 - The Service Hierarchy • 3-8
 - The Signature Editor Console • 12-15
 - The Signature Editor Tool • 4-19
 - The SM GUI Tool • 11-1
 - The Subscriber Manager GUI Tool • 4-20
 - Time-Based Rule • 6

- Time-Based Rules • 3-11
- Traffic Accounting and Reporting • 3-7
- Traffic Classification • 3-1
- Traffic Control • 3-10
- Traffic Discovery Reports • 6
- Traffic Filters • 3-16
- Traffic Forwarding to VAS Servers • 3-16
- Traffic Processing Overview • 3-1
- Transaction (also called Session) • 6
- Traps • 13-12
- Troubleshooting the Protocol Pack
 - Installation • 4-13

U

- Unknown Subscriber Traffic • 3-10, 9-10
- Updating Protocols • 4-9
- Upgrading from Version 2.5 to Version 3.0 • 4-13
- Upgrading the SCA BB Service
 - Configuration Utility • 4-14
- Upstream traffic • 6
- Usage Accounting • 3-7
- User Authentication • 5-29
- Using the Network Navigator • 5-1
- Using the SCA BB Service Configuration Utility • 13-1
- Using the SCA BB Signature Configuration Utility • 13-4
- Using the SCAS BB Console • 4-16
- Using the Service Configuration Editor • 6-1
 - Additional Options • 10-1
 - Traffic Accounting and Reporting • 8-1
 - Traffic Classification • 7-1
 - Traffic Control • 9-1
- Using the Signature Editor • 12-1
- Using the Subscriber Manager GUI Tool • 11-1

V

- Validating the Current Service
 - Configuration • 6-13
- VAS Traffic Forwarding and Bandwidth Management • 10-23
- Verifying the Installation of a Protocol Pack • 4-12
- Verifying Version Compatibility for Protocol Packs • 4-9
- Viewing Calendars • 9-26
- Viewing Current Dynamic Signatures Information • 7-33

- Viewing Filter Rules • 10-2
- Viewing Flavors • 7-48
- Viewing Global Controller Settings • 9-31
- Viewing Packages • 9-2
- Viewing Protocols • 7-21
- Viewing Services • 7-2
- Viewing Subscriber Notifications • 10-11
- Viewing the Rules of a Package • 9-11
- Viewing VAS Traffic Forwarding Tables • 10-26
- Viewing Zones • 7-42

W

- Working with Network Navigator
 - Configuration Files • 5-24
- Working with Subscriber CSV Files • 11-5
- World Wide Web • xii

Z

- Zone Item • 3-6
- Zones • 3-5