

Cisco Service Control Application for Broadband (Cisco SCA BB) User Guide

First Published: September 23, 2015

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

© 2015-2016 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Introduction xxi

Document Revision History xxii

Document Organization xxv

Related Publications xxvi

Obtaining Documentation and Submitting a Service Request xxvi

CHAPTER 1

Cisco Service Control Solution Overview 1

Cisco Service Control Solution 1

Service Control for Broadband Service Providers 2

Cisco Service Control Capabilities 2

Cisco SCE Platform Description 3

Management and Collection 4

Network Management 5

Subscriber Management 5

Service Configuration Management 6

Data Collection 6

CHAPTER 2

Cisco SCA BB System Overview 7

System Components 7

Subscribers and Subscriber Modes 9

Subscriberless Mode 10

Anonymous Subscriber Mode 10

Static Subscriber Mode 11

Subscriber-Aware Mode 11

Subscriber Modes--Summary 12

Service Configuration 13

The Cisco SCA BB Console 14

The Service Configuration Utility 14
The Service Configuration API 14

CHAPTER 3 Introduction to Traffic Processing 17
Routing Environment 17
Traffic Processing 18
Traffic Classification 18
Services 19
Service Elements 20
Examples of Services 21
Protocols 21
Easy Definition of Port-Based Protocols 21
Protocol Elements 22
Signatures 22
Initiating Side 23
Zones 23
Zone Items 24
Flavors 24
Flavor Items 24
DSCP ToS 25
Content Filtering 25
Flow Attributes to Services Mapping 26
Traffic Accounting and Reporting 26
Usage Accounting 26
The Service Hierarchy 27
The Package Hierarchy 27
Reporting 28
Raw Data Records (RDRs) 29
NetFlow 29
Traffic Control 29
Packages 30
Virtual Links Mode 30
Unknown Subscriber Traffic 30
Rules 30
Calendars 31

Bandwidth Management 31
Global Bandwidth Control 31
Subscriber Bandwidth Control 32
Quota Management 34
Subscriber Notification 35
Service Security 35
Detecting Malicious Traffic 36
Responding to Malicious Traffic 36
Traffic Filters 37
DSCP ToS Marking 37
Traffic Forwarding to Value-Added Services Servers 37
Service Configurations 38
Defining Service Configurations in Practice 38

CHAPTER 4 **Getting Started with Cisco SCA BB Console 39**
How to Install Cisco SCA BB 39
The Cisco SCA BB Installation Package 40
Installing Cisco SCA BB Application Components 40
Prerequisites 41
Verifying that the SCE Platform is Operational 41
Verifying that the SCE Platform is Running an Appropriate Version of the OS 41
Verifying that the Subscriber Manager is Correctly Installed 41
Verifying that an Appropriate Version of the Subscriber Manager is Running 41
How to Install Cisco SCA BB Front Ends 42
Cisco SCA BB Hardware Requirements 42
Cisco SCA BB Operating System Requirements 42
Installing the Java Runtime Environment 42
Installing the Cisco SCA BB Console 43
Installing the Cisco SCA BB Configuration Utilities 43
How to Upgrade Cisco SCA BB Components 44
Upgrading the SCE Using the SCE Software Upgrade Wizard 44
Working with Protocol Packs 55
Protocol Packs 55
Installing Protocol Packs 56
How to Install the Service Hierarchy Tree 57

Viewing and Installing the Service Hierarchy Tree 58
Removing the Service Hierarchy Tree 61
Verifying Version Compatibility for Protocol Packs 62
Verifying the Installation of a Protocol Pack 63
Causes for Protocol Pack Installation Failure and Remedies 63
Hitless Upgrade of the SLI 63
Hitless Upgrade CLI Commands 64
Description of Hitless Upgrade CLI Commands 65
Entering Line Interface Configuration Mode 66
Launching the Cisco SCA BB Console 66
How to Use the Cisco SCA BB Console 68
Cisco SCA BB Configuration Wizards 69
Using the Usage Analysis Wizard 70
Using the P2P Traffic Optimization Wizards 81
The Network Navigator Tool 94
Opening the Network Navigator Tool 95
Closing the Network Navigator Tool 95
The Service Configuration Editor Tool 96
Opening the Service Configuration Editor Tool 96
Closing the Service Configuration Editor Tool 98
The Signature Editor Tool 98
Opening the Signature Editor Tool 99
Closing the Signature Editor Tool 99
The Subscriber Manager GUI Tool 99
Opening the Subscriber Manager GUI Tool 100
Closing the Subscriber Manager GUI Tool 100
The Anonymous Group Manager Tool 100
Opening the Anonymous Group Manager Tool 101
Closing the Anonymous Group Manager Tool 101
Online Help 101
Accessing the Online Help 102
Searching Online Help 102
QuickStart with the Cisco SCA BB Console 103
Configuring the Console and Applying the Default Service Configuration 104

CHAPTER 5

The Network Navigator 107

The Network Navigator Tool 107

Introduction to Managing Sites 108

Adding a Site to the Site Manager 108

Introduction to Adding Devices to a Site 109

Adding Cisco SCE Devices to a Site 109

Adding Subscriber Manager Devices to a Site 110

Adding Collection Manager Devices to a Site 111

Deleting Devices 111

Deleting Sites 111

Introduction to Managing Devices 112

Password Management 112

Introduction to Managing Cisco SCE Devices 112

Configuring Cisco SCE and Collection Manager Devices Using a Wizard 112

Generating Tech Support Info Files for Cisco SCE Devices 120

Retrieving the Online Status of Cisco SCE Devices 121

Installing a Protocol Pack on a Single Cisco SCE Platform 123

Introduction to Applying Service Configurations to Cisco SCE Devices 124

Applying a Service Configuration to Multiple Cisco SCE Platforms 124

Applying a Service Configuration to a Single Cisco SCE Platform 125

Introduction to Retrieve Service Configurations from Cisco SCE Devices 126

Retrieving Service Configurations from Multiple Cisco SCE Platforms 126

Retrieving Service Configurations from a Single Cisco SCE Platform 126

Installing PQI Files on Cisco SCE Devices 126

Installing a Cisco SCE OS Software Package on Cisco SCE Devices 128

Introduction to Managing Subscriber Manager Devices 129

Generating Tech Support Info Files for Subscriber Manager Devices 129

Retrieving the Online Status of Subscriber Manager Devices 130

Connecting to Subscriber Manager Devices 131

Introduction to Managing Collection Manager Devices 131

Retrieving the Online Status of CM Devices 131

Working with Network Navigator Configuration Files 132

Exporting a Network Navigator Configuration 132

Importing a Network Navigator Configuration 135

Network Settings Requirements 137
Firewall and NAT Requirements 137
User Authentication 137
Introduction to Disabling PRPC Authentication 138
Disabling PRPC Authentication on a Cisco SCE Platform 138
Disabling PRPC Authentication on a CM 138
Disabling PRPC Authentication on an Subscriber Manager 139

CHAPTER 6 Using the Service Configuration Editor 141
Service Configurations 141
Managing Service Configurations 141
Opening the Service Configuration Editor Tool 142
Adding New Service Configurations 142
Opening Existing Service Configurations 144
How to Save the Current Service Configuration 145
Saving the Current Service Configuration to a Service Configuration File 145
Saving the Current Service Configuration to the File from Which it Was Loaded 146
Closing Service Configurations 146
Exporting Service Configuration Data 147
Importing Service Configuration Data 150
How to Apply and Retrieve Service Configurations 154
Validating the Current Service Configuration 154
Applying a Service Configuration to SCE Platforms 155

CHAPTER 7 Traffic Classification Using Service Configuration Editor 157
Searching Traffic Classification Settings 157
Introduction to Managing Services 158
Service Parameters 159
How to Add and Define Services 160
Adding a Service to a Service Configuration 160
Defining Hierarchical Settings for a Service 161
Setting the Service Index 162
Viewing Services 163
Editing Services 165
Deleting Services 166

Introduction to Managing Service Elements 167
Adding Service Elements 168
Duplicating Service Elements 172
Editing Service Elements 173
Deleting a Service Element 175
Moving Service Elements 176
Introduction to Managing Protocols 177
Viewing Protocols 178
Filtering a Protocols List 179
Adding Protocols to a Service Configuration 180
Editing Parameters of a Protocol 181
Deleting Protocols 182
Introduction to Managing Protocol Elements 183
Adding Protocol Elements 184
Editing Protocol Elements 187
Deleting Protocol Elements 188
Introduction to Managing Zones 189
BGP Autonomous System Dynamic Detection 189
Viewing Zones 189
Adding Zones 190
Editing Zones 193
Deleting Zones 193
Introduction to Managing Zone Items 194
Adding Zone Items 194
Editing Zone Items 195
Deleting Zone Items 196
BGP AS Dynamic Detection Workflow 196
Enabling BGP As Dynamic Detection 196
Collecting and Storing the BGP Autonomous System Details 197
Creating a New Zone with Select BGP AS Numbers and Prefixes 198
BGP AS Numbers and Prefixes Color Schema 199
Updating a Zone with Select BGP AS Numbers and Prefixes 200
Deleting IP Prefixes from a Zone 200
Introduction to Managing Protocol Signatures 200
Viewing Protocol Signatures 200

Filtering the Protocol Signatures List 201
Dynamic Signatures 202
Dynamic Signature Script Files 203
Viewing Information About the Current Dynamic Signatures 203
Importing a Dynamic Signature Script into a Service Configuration 205
Removing Dynamic Protocol Signatures 206
The Default DSS File 207
Introduction to Setting and Clearing the Default DSS File 208
Setting a Protocol Pack as the Default DSS File 208
Clearing the Default DSS File 210
Introduction to Importing Dynamic Signatures from the Default DSS File 211
Importing the Default DSS File Automatically 211
Importing the Default DSS File Manually 211
Introduction to Managing Flavors 213
Flavor Types and Parameters 213
Viewing Flavors 216
Adding Flavors 218
Adding 2M URL support 220
Editing Flavors 222
Deleting Flavors 222
Introduction to Managing Flavor Items 223
Maximum Number of Flavor Items per Flavor Type 224
Adding Flavor Items 224
Editing Flavor Items 226
Deleting Flavor Items 227
Example on How to Import a List of URLs and Block Them 227
Introduction to Managing Content Filtering 228
Information About Content Filtering 228
The Cisco SCE Application 228
The Cisco CPA Client 229
The SurfControl CPA Server 229
The Content Filtering CLI 229
CPA Client CLI Commands 229
Description of CPA Client CLI Commands 229
Configuring the RDR Formatter 230

Entering Line Interface Configuration Mode 231
Managing Content Filtering Settings 231
Importing Content Filtering Categories 232
HTTP Content Category Flavors 233
HTTP Browsing with Categories Service Elements 234
Importing Content Filtering Categories Using the Import Dialog Box 234
Importing Content Filtering Categories Using the HTTP Content Filtering Settings Dialog Box 238
Enabling Content Filtering 239
Viewing Content Filtering Settings 240
Configuring Content Filtering 241
Example for How to Configure Content Filtering for Web Based E-mail 241
Removing Content Filtering Settings 242
OS Fingerprinting Overview 243
Enabling OS Fingerprinting 244
Installing OS Fingerprinting Signatures 246
Viewing Subscriber OS Information 246
Disabling OS Fingerprinting 247
The OS Fingerprinting CLI 247
Configuring Policy for DNS Assisted Classification 247

CHAPTER 8 **Traffic Accounting and Reporting Using the Service Configuration Editor 251**
Usage Counters 251
Raw Data Records 252
NetFlow Records 252
Managing RDR Settings 252
The RDR Settings Dialog Box 252
Managing Usage RDRs 253
Managing Transaction RDRs 256
Managing Quota RDRs 258
Managing Transaction Usage RDRs 260
Managing Log RDRs 262
Managing Real-Time Subscriber Usage RDRs 264
Managing Real-Time Signaling RDRs 266

CHAPTER 9 Traffic Control Using the Service Configuration Editor 269

Introduction to Managing Bandwidth 269

Managing Global Bandwidth Overview 270

Viewing Global Controller Settings 270

Filtering Global Controllers 272

Editing the Total Link Limits 273

Introduction to Defining Global Controllers 274

Setting Global Controller Bandwidth Limits Separately with a Different Rate Per Link 275

Setting Global Controller Bandwidth Limits as the Sum of All Links with a Different Rate Per Link 278

Setting Global Controller Bandwidth Limits as the Sum of All Links with an Equal Rate Per Link 281

Setting Global Controller Bandwidth Limits with Equal Rate for All Links 284

Setting Global Controller Bandwidth for Virtual Links 287

Introduction to Managing Subscriber Bandwidth 291

Subscriber BWC Parameters 291

Editing Package Subscriber BWCs 292

A Practical Example of Managing Bandwidth 294

Configuring Total Bandwidth Control 295

Example for Limiting P2P and Streaming Traffic Using the Console 295

Configuring a Rule, Bandwidth Controller, and Global Controller Using the Wizard 300

Configuring the Upstream Configuration of the Global Bandwidth Controller for IPv6 303

Setting Bandwidth Management Prioritization Mode 304

Introduction to Managing Virtual Links 305

Collection Manager Virtual Links Names Utility 306

Enabling Virtual Links Mode 306

Viewing Virtual Links Global Controller Settings 307

Managing Virtual Links Global Controllers 310

Adding Global Controllers 310

Setting the Maximum Bandwidth of Global Controllers 313

Deleting Global Controllers 314

Configuring a Service Configuation in Virtual Links Mode 315

Editing the Virtual Links Total Link Limits 316

Managing Virtual Links with CLI Commands 316
Description of Virtual Links CLI Commands 317
Entering Line Interface Configuration Mode 317
Introduction to Managing Packages 318
Package Parameters 318
Viewing Packages 319
Adding Packages 320
Setting Advanced Package Options 322
Duplicating Packages 324
Editing Packages 324
Deleting Packages 325
Introduction to Add-on Packages 326
Adding Add-on Groups 327
Adding Add-on Template 329
Package Combinations 330
Creating a Package Combination 330
Introduction to Managing Rules 331
The Default Service Rule 332
Rule Hierarchy 332
Viewing the Rules of a Package 332
Adding Rules to a Package 333
Defining Per-Flow Actions for a Rule 335
Editing Rules 337
Deleting Rules 339
Displaying the Services Affected by a Rule 339
Global Rules 340
Adding Global Rules 340
Editing a Global Rule 342
Adding Additional Global Rules for a Service 344
Deleting a Global Rule from a Service 346
Deleting All Additional Rules from a Service 346
Adding a Global Rule to a Package 347
Deleting a Global Rule from a Package 348
Displaying Packages Associated to a Global Rule 349
Time-Based Rules Overview 350

Adding Time-Based Rules to a Rule 350
Editing Time-Based Rules 352
Deleting Time-Based Rules 353
Managing Calendars Overview 353
Adding Calendars 354
Renaming the Time Frames 354
Viewing Calendars 355
Deleting Calendars 356
Configuring the Time Frames 357
How to Manage DSCP ToS Marker Values 358
Configuring DSCP ToS Marking 359
Quota Management 360
Adding Quota Profiles 360
Editing Quota Profiles 362
Deleting Quota Profiles 368
Editing Quota Management Settings for Packages 368
Quota Replenish Scatter 369
Selecting Quota Buckets for Rules 370
Editing Breach-Handling Parameters for a Rule 373
Breach-Handling Parameters 375
Example for Creating Tiered Subscriber Services 376
Unknown Subscriber Traffic 377

CHAPTER 10 **Service Configuration Editor: Additional Options** 379
The Service Security Dashboard 379
Viewing the Service Security Dashboard 380
Introduction to Managing Worm Detection 380
Viewing Supported Worm Signatures 380
Adding New Worm Signatures to a Service Configuration 381
Managing Anomaly Detection Overview 381
Anomaly Detection 381
Anomaly Detection Parameters 382
Viewing Anomaly Detection Settings 384
Adding Anomaly Detectors 386
Editing Anomaly Detectors 390

Editing Detector Parameters 391
Editing Anomaly Types 391
Adding an Anomaly Type 392
Deleting an Anomaly Type 393
Changing the Order in which Detectors are Checked 393
Deleting Anomaly Detectors 394
Managing Spam Detection Overview 394
Configuring Spam Detection Settings 395
Configuring Outgoing Spam Mitigation Settings per Package from Subscriber Policies 397
Malicious Traffic Reports Overview 398
Malicious Traffic Reports 398
Viewing a Service Security Report 399
Traffic Flow Filtering 399
Information About Traffic Filtering 400
The Cisco SCA BB Filtered Traffic Mechanism 400
Filter Rule Actions 401
Filter Rules and Service Rules 402
Automatic Quick Forwarding of Media Flows 402
Filtering L2TP Traffic 402
Viewing Filter Rules for a Package 402
Setting Flexible Configuration of Port based Filters 403
Adding Filter Rules 404
Adding Filter Rules for IPv6 Configuration 409
Editing Filter Rules 415
Deleting Filter Rules 415
Activating and Deactivating Filter Rules 416
Managing Subscriber Notifications Overview 416
Subscriber Notification Parameters 417
Network Attack Notification 419
Network Attack Notification Parameters 419
Example of URL with Description Tail 420
Adding a Notification Redirect Profile 420
Managing Subscriber Redirection Overview 424
Subscriber Redirect Parameters 424
Adding a Redirect Profile 426

Deleting a Redirection Profile 430
Adding a Set of Redirection URLs 430
Deleting a Set of Redirection URLs 433
Managing the System Settings Overview 433
System Operational Mode 434
Setting the Operational and Topological Modes of the System 434
Asymmetric Routing Classification Mode 434
Advanced Service Configuration Options 435
The Advanced Service Configuration Properties 435
Editing Advanced Service Configuration Options 443
Managing VAS Settings Overview 444
Enabling VAS Traffic Forwarding 445
Enabling VAS Traffic Mirroring 446
Renaming VAS Server Groups 447
Configuring VAS Traffic-Mirroring 449
Viewing VAS Traffic-Forwarding Tables 450
Deleting VAS Traffic-Forwarding Tables 451
Adding VAS Traffic-Forwarding Tables 451
Managing VAS Table Parameters Overview 453
Adding VAS Table Parameters 453
Editing VAS Table Parameters 454
Deleting VAS Table Parameters 455
Managing the Protected URL Database 456

CHAPTER 11 **Subscriber Manager GUI Tool** 457
Subscriber Manager GUI Tool Overview 457
Connecting to a Cisco Service Control Subscriber Manager Overview 458
Connecting to a Cisco Service Control Subscriber Manager from the Network Navigator 458
Connecting to a Cisco Service Control Subscriber Manager from the Console 459
Disconnecting from the Current Cisco Service Control Subscriber Manager 460
Subscriber CSV Files Overview 461
Importing Subscriber Information from a CSV File 461
Exporting Subscriber Information to a CSV File 462
Subscriber Management Overview 462

Subscriber Information 463
Overview of How to Find and Select Subscribers 465
Finding a Subscriber or Group of Subscribers 465
Selecting Subscribers 466
Selecting a Range of Subscribers 466
Selecting a Number of Noncontiguous Subscribers 466
Adding a Subscriber 467
Editing Subscriber Details 468
Deleting a Subscriber from the Database 470
Monitoring SM Online Status 471

CHAPTER 12 Anonymous Group Manager GUI Tool 473
Using the Anonymous Group Manager GUI Tool 473
Introduction to Managing Anonymous Groups 474
Anonymous Group Manager Information 474
Finding and Selecting Subscribers Overview 475
Selecting Subscribers Overview 477
Selecting a Range of Subscribers 477
Selecting a Number of Noncontiguous Subscribers 477
Adding a Cisco SCE to the Anonymous Group Manager GUI Tool 478
Adding a New Anonymous Group in a Cisco SCE Device 478
Adding a New IPv6 Anonymous Group in a Cisco SCE Device 479
Viewing the Configuration of a Specific Anonymous Group 480
Deleting An Anonymous Groups in a Cisco SCE 481
Deleting All Anonymous Groups in a Cisco SCE 481
Viewing Subscribers in a Specific Anonymous Group 482
Viewing the Online Status of a Subscriber 483
Editing the Subscriber Properties 484
Removing Subscribers from an Anonymous Group in a Cisco SCE 484
Working with Anonymous Groups CSV Files 484
Exporting Anonymous Groups to a CSV File 487
Exporting Information on Subscribers of an Anonymous Group to CSV File 489

CHAPTER 13 The Signature Editor Overview 491
The Signature Editor Console 491

Managing DSS Files Overview 491
The DSS File Components 492
The DSS File 492
DSS Protocol List 492
Information About DSS Protocols 492
DSS Protocol Name and ID 493
DSS Buddy Protocol 494
DSS Signatures 494
DSS String Match Signature 494
DSS Payload Length Signature 496
DSS HTTP User Agent Signature 498
DSS HTTP x-Header Signature 499
DSS Deep Inspection Clauses 499
DSS Deep Inspection Conditions 500
Creating DSS Files 502
Editing DSS Files 504
Importing DSS Files 505

CHAPTER 14 **Additional Management Tools and Interfaces 509**
The Cisco SCA BB Service Configuration Utility 509
servconf Syntax 509
servconf Examples 512
The Cisco SCA BB Signature Configuration Utility 513
sigconf Syntax 513
sigconf Examples 513
Overview of SNMP, MIB, and Traps 514
SNMP 514
MIB 514
Traps 514
Installing a Cisco SCA BB PQI File on a Cisco SCE Platform 515
Entering Line Interface Configuration Mode 515
Overview on Managing Subscribers via Other System Components 515
Anonymous Subscriber Mode 516
Subscriber-Aware Mode 517
The Cisco SCE Platform Subscriber CLI 517

The SM Subscriber Management CLU 518
Selecting Subscribers for Real-Time Usage Monitoring 519
Managing Subscriber Monitoring via the SM 519
Enabling Subscriber Monitoring for a Subscriber via the SM 519
Disabling Subscriber Monitoring for a Subscriber via the SM 519
Enabling Subscriber Monitoring for Multiple Subscribers 519
Verifying that Subscriber Monitoring is Enabled for a Subscriber via the SM 520
Managing Subscriber Monitoring via the Cisco SCE Platform Overview 520
Enabling Subscriber Monitoring for a Subscriber 520
Disabling Subscriber Monitoring for a Subscriber 520
Enabling Subscriber Monitoring for Multiple Subscribers 521
Verifying that Subscriber Monitoring is Enabled for a Subscriber 521
Managing Subscriber CSV Files 521
Importing Subscriber CSV Files 522
Exporting Subscriber CSV Files 522
Filtering and Exporting Subscribers Example 522



Introduction

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

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

- Document Revision History, page xxii
- Document Organization, page xxv
- Related Publications, page xxvi
- Obtaining Documentation and Submitting a Service Request, page xxvi

Document Revision History

Revision	Cisco Service Control Release and Date	Change Summary
OL-31908-01	Release 4.2.x August 26, 2014	First version of this document (new for the release 4.2.x train). Release 4.2.0 updates: • Added details about Package-ID to Package-Name Mapping in the Subscriber Information. • Updated the HTTP URL and HTTP Referer in the Flavor Types and Parameters . • Included the IPv6 filter rules for a package in Viewing Filter Rules for a Package . • Updated the flavors support in asymmetrical mode in the Managing the System Settings Overview. • Support of IPV6 address in the anomaly attack detection. See Adding Anomaly Detectors , on page 386section. • Removed references to SCE 1000, SCE 2000. • Removed references to Solaris.

Revision	Cisco Service Control Release and Date	Change Summary
OL-31849-01	Release 5.0.x July 30, 2014	First version of this document (new for the release 5.0.x train). Release 5.0.0 updates: • Telnet Support. See Establishing Telnet Session for Devicessection. • Support of Incremental Apply Policy. See Applying Zones and Flavors • Updated information to configurable PRPC port . • Windows 64 bit support in the Cisco SCA BB Operating System Requirements . • Increased Global and Subscriber Usage Counter values in the Defining Hierarchical Settings for a Service , on page 161 section. • Support of IPV6 address in the anomaly attack detection. See Adding Anomaly Detectors , on page 386section. • Removed references to SCE 1000, SCE 2000. • Removed references to Solaris.

Revision	Cisco Service Control Release and Date	Change Summary
-	Release 5.1.x February 18, 2015	Release 5.1.0 updates: • Updated Applying Zones and Flavors section. • Updated User Authentication section. • Updated Opening Existing Service Configurations section. • Updated Maximum Number of Flavor Items per Flavor Type section. • Added Configuring Policy for DNS Assisted Classification section. • Updated Introduction to Managing Packages section. • Added Introduction to Add-on Packages section. • Updated Setting Flexible Configuration of Port based Filters section. • Removed references to SCE 1000, SCE 2000. • Removed references to Solaris.

Revision	Cisco Service Control Release and Date	Change Summary
-	Release 5.2.x September 20, 2015	Release 5.2.0 updates: • Removed references to SCE 10000 and vSCE. • Added "Hide Subscriber IP and ID in RDRs with Empty String" field in Table 13: Advanced Service Configuration Properties.

Document Organization

Section	Title	Description
Chapter 1	Cisco Service Control Overview	Provides a general overview of the Cisco Service Control solution.
Chapter 2	System Overview	Provides a functional overview of the Cisco Service Control solution.
Chapter 3	Traffic Processing Overview	Provides a technical overview of the Cisco Service Control solution.
Chapter 4	Getting Started	Guides you through the process of installing or upgrading Cisco SCA BB and describes the concept of the Console as a collection of tools.
Chapter 5	Using the Network Navigator	Explains how to use the Network Navigator to create a model of all devices that are part of the Cisco Service Control solution and how to manage the devices remotely.
Chapter 6	Using the Service Configuration Editor	Explains how to use the Service Configuration Editor to manage service configurations.
Chapter 7	Using the Service Configuration Editor: Traffic Classification	Explains how to configure service configurations to perform traffic classification.
Chapter 8	Using the Service Configuration Editor: Traffic Accounting and Reporting	Explains how to configure service configurations to perform traffic reporting.
Chapter 9	Using the Service Configuration Editor: Traffic Control	Explains how to configure service configurations to perform traffic control.
Chapter 10	Using the Service Configuration Editor: Additional Options	Documents additional, advanced options available in the Service Configuration Editor.
Chapter 11	Using the Subscriber Manager GUI Tool	Explains how to use the Subscriber Manager GUI tool to configure subscribers on the Cisco Service Control Subscriber Manager database.

Section	Title	Description
Chapter 12	Using the Anonymous Group Manager Tool	Explains how to use the Anonymous Group Manager GUI tool to configure the anonymous groups and subscribers in Cisco SCEs.
Chapter 13	Using the Signature Editor	Documents the Signature Editor tool, which can create files for updating protocols in Cisco SCA BB.
Chapter 14	Additional Management Tools and Interfaces	Documents and explains other tools that are available for use with Cisco SCA BB.

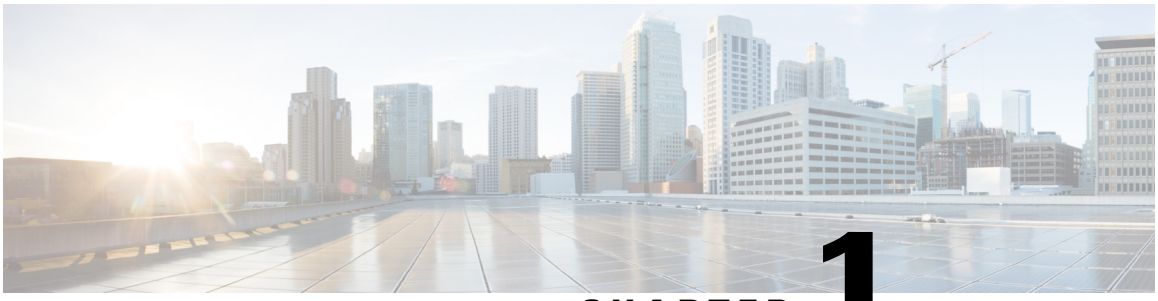
Related Publications

- Cisco Service Control Application for Broadband Reference Guide
- Cisco Service Control Application for Broadband Service Configuration API Programmer Guide
- Cisco Service Control Management Suite Collection Manager User Guide
- Cisco Service Control Management Suite Subscriber Manager User Guide
- Cisco Insight User Guide
- Cisco Service Control Mobile Solution Guide
- Cisco Service Control Usage-Based Services Solution Guide
- Cisco Service Control for Managing Remote Cable MSO Links Solution Guide
- The Cisco SCE platform installation and configuration guides:

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



CHAPTER 1

Cisco Service Control Solution Overview

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

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

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

Cisco Service Control Solution

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

Service control enables service providers to:

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

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

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

Service Control for Broadband Service Providers

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

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

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

Cisco Service Control Capabilities

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

- Subscriber and application awareness—Application-level drilling into IP traffic for real-time understanding and controlling of usage and content at the granularity of a specific subscriber.
  - Subscriber awareness—The ability to map between IP flows and a specific subscriber to maintain the state of each subscriber transmitting traffic through the Cisco SCE platform and to enforce an appropriate policy on this subscriber's traffic.
    Subscriber awareness is achieved either through dedicated integrations with subscriber management repositories, such as a DHCP or a RADIUS server, or through sniffing of RADIUS or DHCP traffic.
  - Application awareness—The ability to understand and analyze traffic up to the application protocol layer (Layer 7).
    For application protocols implemented using bundled flows (such as FTP, which is implemented using Control and Data flows), the Cisco SCE platform understands the bundling connection between the flows and treats them accordingly.
- Application-layer, stateful, real-time traffic control—The ability to perform advanced control functions, including granular bandwidth (BW) metering and shaping, quota management, and redirection, using application-layer, stateful, real-time traffic transaction processing. This feature requires highly adaptive protocol and application-level intelligence.

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

Cisco SCE Platform Description

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

The Cisco SCE platform devices:

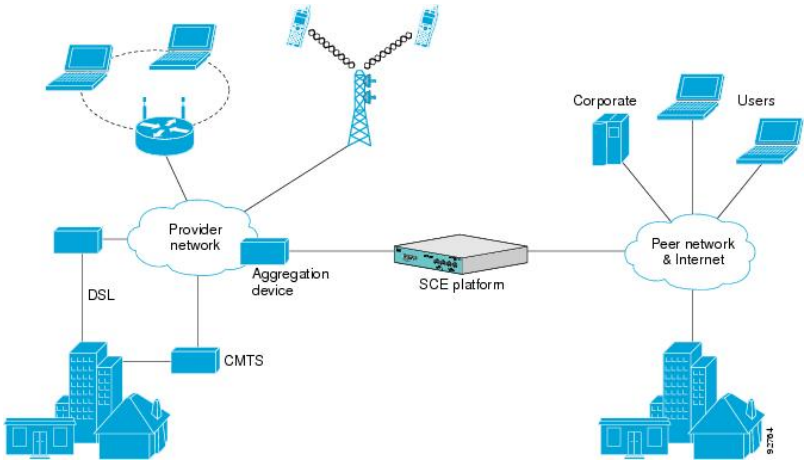
- Are programmable.
- Provide stateful inspection of bidirectional traffic flows, and mapping these flows with user ownership.
- Provide real-time classification of network use. The classification provides the basis of the Cisco SCE platform advanced traffic-control and bandwidth-shaping functionality.

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

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

- Subscriber awareness that relates traffic and usage to specific customers

Figure 1: Common Deployment of a Cisco SCE Platform in a Network



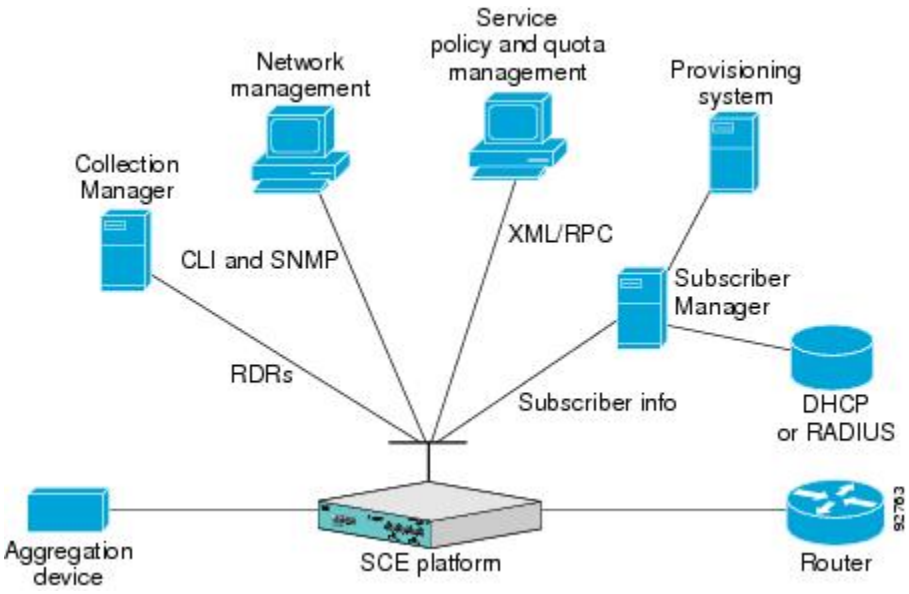
Management and Collection

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

- Network management
- Subscriber management
- Service Control management

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

Figure 2: Service Control Management Infrastructure



Network Management

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

Two interfaces provide network management:

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

Subscriber Management

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

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

Subscriber information may be obtained in one of two ways:

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

Service Configuration Management

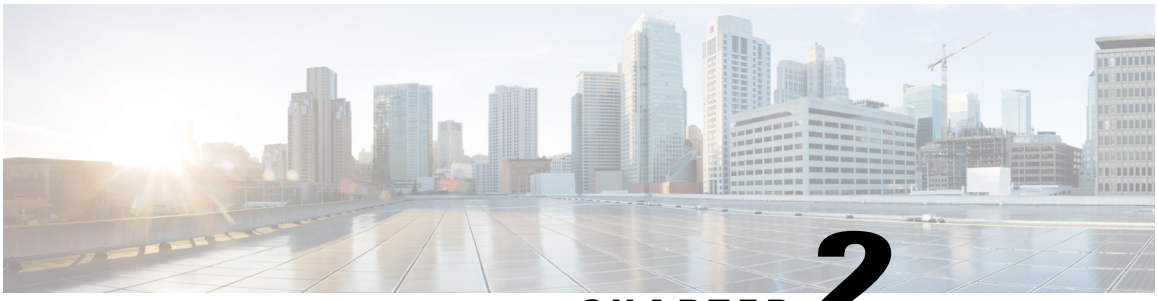
Service configuration management is the ability to configure the general service definitions of a service control application. A service configuration file containing settings for traffic classification, accounting and reporting, and control is created and applied to a Cisco SCE platform. The Cisco SCA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

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

Data Collection

Data collection occurs as follows:

1. Cisco SCE Platform analyzes and process the data passing through it and generates Raw Data Records (RDRs).
2. Cisco SCE Platform then forwards these RDRs to Cisco service control management suite collection manager using a simple TCP-based protocol (RDR-Protocol).
   The collection manager software is an implementation of a collection system that receives RDRs from one or more Cisco SCE platforms.
3. The collection manager collects these records and processes them in one of its adapters. Each adapter performs a specific action on the RDR.
   RDRs contain various information and statistics, depending on the configuration of the system. The main categories of RDRs include:
   - Transaction RDRs—Records generated for each *transaction* , where a transaction is a single event detected in network traffic. The identification of a transaction depends on the particular application and protocol.
   - Subscriber Usage RDRs—Records generated per subscriber, describing the traffic generated by that subscriber for a defined interval.
   - Link RDRs—Records generated per link, describing the traffic carried on the link for a defined interval.
   - Zone RDRs—Records generated per zone, describing the traffic carried on the zone for a defined interval.



CHAPTER 2

Cisco SCA BB System Overview

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

- System Components, page 7
- Subscribers and Subscriber Modes , page 9
- Service Configuration , page 13

System Components

The Cisco Service Control solution consists of four main components:

- The Cisco Service Control Engine (Cisco SCE) platform—A flexible and powerful dedicated network-usage monitor that is purpose-built to analyze and report on network transactions at the application level.
  For more information about the installation and operation of the Cisco SCE platform, see the *Cisco SCE Platform Installation and Configuration Guides* .
- The Cisco Service Control Subscriber Manager—A middleware software component that is used where dynamic binding of subscriber information and policies are required. The Subscriber Manager manages subscriber information and provisions it in real time to multiple Cisco SCE platforms. The Subscriber Manager can store subscriber policy information internally, and act as a stateful bridge between the AAA system (such as RADIUS and DHCP) and the Cisco SCE platforms.
  For more information about the installation and operation of the Subscriber Manager, see the *Cisco Service Control Management Suite Subscriber Manager User Guide.*

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

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

- The Cisco Service Control Collection Manager (CM)—An implementation of a collection system that receives Raw Data Records (RDRs) from one or more Cisco SCE platforms. It collects usage information and statistics, and stores them in a database. The CM also converts subscriber usage information and statistics into simple text-based files for further processing and collection by external systems.
  For more information about the installation and operation of the CM, see the *Cisco Service Control Management Suite Collection Manager User Guide.*
- The Service Control Application (SCA) Reporter—A software component that processes data stored by the CM and provides a set of insightful reports from this data. The SCA Reporter can run as a standalone or as an integrated part of the Console.
  For more information about the installation and operation of the Reporter, see the *Cisco Service Control Application Reporter User Guide.*

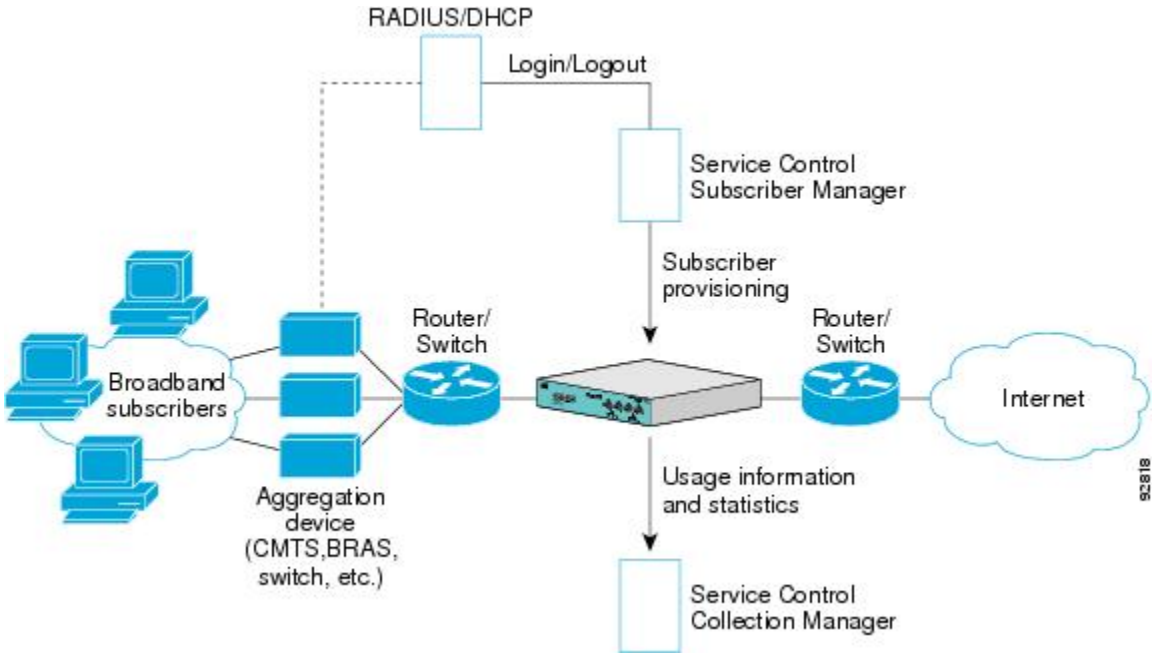
Together, the Cisco SCE platform, the Cisco Service Control Collection Manager, the Cisco Service Control Subscriber Manager, and the SCA Reporter are designed to support detailed classification, analysis, reporting, and control of IP network traffic. The Cisco Service Control Collection Manager, the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

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

- Horizontal flow—Represents traffic between subscribers and an IP network.
  The Cisco SCE platform monitors traffic flow.
- Vertical flow—Represents transmission of the Raw Data Records (RDRs) from the Cisco SCE platform to the CM.

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

Figure 3: Flow of Information in Cisco SCA BB



Subscribers and Subscriber Modes

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

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

Cisco SCA BB supports the following four subscriber modes:

- Subscriberless mode—No subscribers are defined. Control and link-level analysis functions are provided at a global platform resolution.
- Anonymous subscriber mode—IP addresses are controlled and monitored individually. The Cisco SCE platform automatically identifies IP addresses as they are used and assigns them to a package.
- Static subscriber mode—Incoming IP addresses are bound and grouped statically into “subscribers” as configured by the system operator.

- Subscriber-aware mode—Subscriber information is dynamically bound to the IP address currently in use by the subscriber. Subscriber-aware mode can be achieved by integrating Cisco SCA BB with the system (RADIUS, DHCP) that assigns IP addresses to subscribers, or by sniffing this information. Policy information is either administered to Cisco SCA BB directly or provisioned dynamically via an integration.

Subscriberless Mode

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

Subscriberless mode requires no integration; hence, the Cisco Service Control Subscriber Manager is not required.



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

Anonymous Subscriber Mode

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

Use this mode when:

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

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

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

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



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

Static Subscriber Mode

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

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

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

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

Subscriber-Aware Mode

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

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

In this mode, the Cisco Service Control Subscriber Manager may provision the Cisco SCE platform with subscriber information.

Subscriber Modes--Summary

Table 1: Summary of Subscriber Modes

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

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

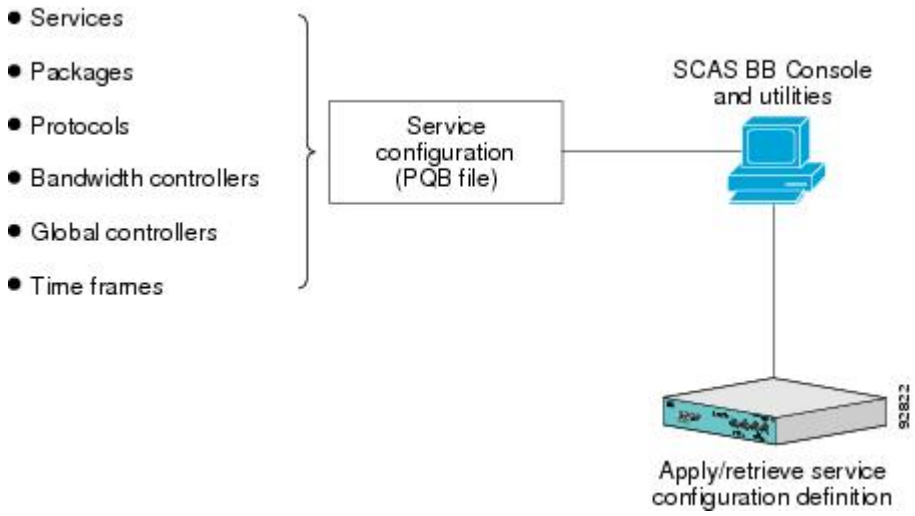
Service Configuration

Service configuration defines the way the Cisco SCE platform analyses and controls traffic. In general terms, service configuration defines the following:

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

- Global controllers

Figure 4: Service Configuration



Service configuration is accomplished using one of the following:

The Cisco SCA BB Console

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

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

The Service Configuration Utility

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

For full documentation of the servconf, see The Cisco SCA BB Service Configuration Utility .

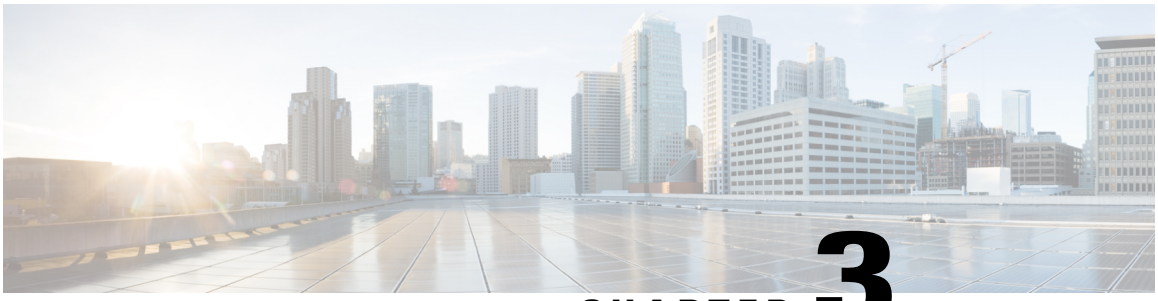
The Service Configuration API

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

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

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

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



CHAPTER 3

Introduction to Traffic Processing

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

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

This chapter consists of these sections:

- Routing Environment , page 17
- Traffic Processing , page 18
- Traffic Classification , page 18
- Traffic Accounting and Reporting , page 26
- Traffic Control , page 29
- Service Security , page 35
- Traffic Filters , page 37
- Traffic Forwarding to Value-Added Services Servers , page 37
- Service Configurations , page 38

Routing Environment

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

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

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

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

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

Traffic Processing

There are three stages of traffic processing:

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

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

The three stages are described in these sections:

Traffic Classification

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

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

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

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

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

- If the packet is UDP, hardware flows are created for first packet in each direction.
- If the packet is UDP, software flow is created for the 5th packet.

Creating flow on the fifth packet helps to avoid creation of software flows for port-scans, and thus, protect Cisco SCE from DoS conditions. Port-scans are still detected because their flows are opened in hardware temporarily. Also, some flows are still opened on the first packet, based on SCA-BB GUI options (Advanced settings).

- If the flow is non-TCP, non-UDP but still IP (for example, ICMP), hardware flow is opened for each direction on first packet
- If the flow is non-TCP, non-UDP but still IP (for example, ICMP), software flow is opened for each direction on second packet

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

Services

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

Services are the building blocks for:

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

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

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

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

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

- Protocol—The protocol used. This classification allows, for example, the mapping of browsing flows and e-mail flows to separate services.
- Initiating side—Whether the subscriber side or the network side generated the flow. This classification allows, for example, the mapping of subscriber-initiated and network-initiated peer-to-peer traffic to separate services.
- Zone—Lists of IP addresses of the network-side host of the flow. This classification allows, for example, the mapping of all voice flows going to a specified server to a specific service.

- Flavor—Specific Layer 7 properties such as host names of the network-side host of the flow. This classification allows, for example, the mapping of all HTTP flows where the URL matches a certain pattern to a specific service.

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

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

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

Service Elements

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

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

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

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

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

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

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

Examples of Services

Table 2: Examples of Services and Service Parameters

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

Protocols

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

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

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

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

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

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

Easy Definition of Port-Based Protocols

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

This assignment is done automatically, so you do not need to do the assignment manually. These protocol-elements that are added automatically are not displayed in the GUI. If, on the other hand, you want

to assign the “Behavioral Upload/Download” signature on a specific port to a different protocol, you can do it by creating an appropriate protocol-element and assigning it to the other protocol.



Note In the default configuration, the HTTP protocol definition accepts not just the HTTP signature, but also all other generic (unclassified) traffic on port 80, by including the protocol-element <“Generic” signature, port 80>. As described previously, when a protocol-element in this form, <“Generic” signature, specific port>, is used in a certain protocol definition, the Cisco SCE maps both the generic and the behavioral signatures, on the specified port, to that protocol. For HTTP traffic, this means that traffic on port 80, which is classified as “Behavioral Upload/Download” signature, would also be assigned to the HTTP protocol. As described earlier, the purpose of this behavior is to allow easy definition of port-based protocols. Nevertheless, this behavior can be avoided, by adding the protocol-element <“Behavioral” signature, specific port> to a different protocol.

Protocol Elements

A protocol is a collection of protocol elements.

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

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

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

If a flow matches two protocol elements and one is more specific than the other, the flow is mapped to the more specific of the two.

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

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

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

Signatures

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

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

When unidirectional classification is enabled and a unidirectional flow (inbound or outbound) passes through the Cisco SCE platform, the flow is matched against a special set of unidirectional protocol signatures. When

a bidirectional flow passes through the Cisco SCE platform, the protocol library tries to match it to one of its standard (bidirectional) protocol signatures.

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

Dynamic Signatures

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

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

Initiating Side

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

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

Zones

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

You configure zones by arranging IP addresses in groups connected by a common purpose. A network flow of the subscriber mapped to a service may be applied to a zone. In practice, zones often define geographical areas.

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

Examples of Zones:

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

Example of Assigning a Zone to a Session:

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

Zone Items

A zone is a collection of related zone items.

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

Table 3: Examples of Zone Items

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

For details on managing zones and zone items, see the Introduction to Managing Zones section.

Flavors

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

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

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

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

Flavor Items

A flavor is a collection of flavor items.

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

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

DSCP ToS

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

Content Filtering

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

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

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

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

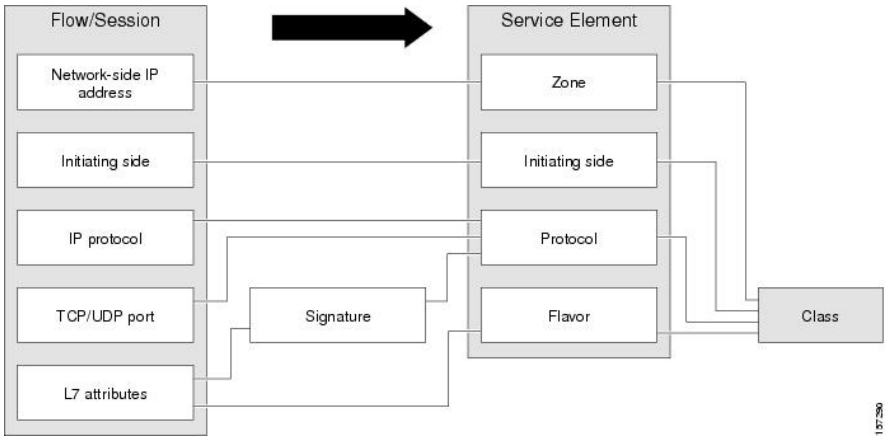


Note Cisco SCA BB includes an internal database of URLs used by the HTTP URL flavor classification. When a URL is found in both the internal database and the external content filtering database, the URL is classified according to the internal database.

Flow Attributes to Services Mapping

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

Figure 5: Mapping Flow Elements of a Session to Service Elements of a Service



Traffic Accounting and Reporting

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

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

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

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

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

Usage Accounting

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

The network metrics are:

- Upstream volume (L3 kilobytes)
- Downstream volume (L3 kilobytes)
- Sessions
- Active subscribers

- Concurrent sessions
- Session duration



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

Per service accounting takes place in the following scopes:

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

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

The Service Hierarchy

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

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

Service Usage Counters

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

There are two categories of usage counters for services:

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

A global usage counter and a subscriber usage counter are assigned to each service. The use of a service can be accounted either exclusively for traffic classified to it or with the traffic of its parent service. For example, if a service called Premium Video Content is defined as a child of Streaming, the operator can either define a special usage counter for Premium Video Content or configure it to use the same usage counter as Streaming.

The global usage counter and the subscriber usage counter are independent. For the same service, one usage counter may be the same for parent and child, whereas the other is exclusive to the child.

The Package Hierarchy

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

Package Usage Counters

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

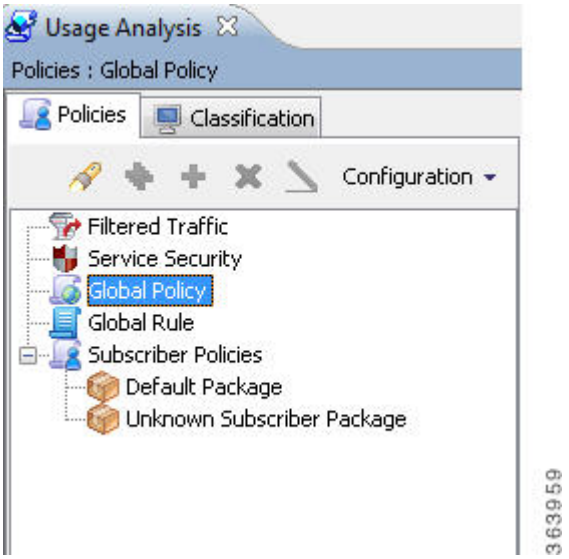
Usage reporting at a package level is grouped as follows:

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

In the figure Example Package Tree, if the Mail & Web Baseline package is allocated an exclusive counter, but neither child package is assigned an exclusive counter, then all Package Usage RDRs and derived reports (such as "Package Bandwidth per Service") would group usage of subscribers assigned to all three packages.

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

Figure 6: Example Package Tree



Reporting

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

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

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

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

This section contains these topics:

Raw Data Records (RDRs)

The following are the main categories of RDRs:

- Usage RDRs—Generated periodically. These RDRs contain the state of the usage counters, per service and per accounting scope. There are four types of usage RDRs:
  - Link Usage RDRs—Global usage per service, for the entire link.
  - Package Usage RDRs—Usage per group of subscribers, per service.
  - Subscriber Usage RDRs—Usage per subscriber, per service. These RDRs are generated for all subscribers. The Cisco Service Control Collection Manager (CM) and Cisco Service Control Application (SCA) Reporter use these RDRs to generate top-subscriber reports and aggregated usage billing records.
  - Real-Time Subscriber Usage RDRs—Generated for selected subscribers only. The Cisco Service Control Collection Manager and SCA Reporter use these RDRs by to generate detailed subscriber activity reports.
- Transaction RDRs—Generated for a sample of the flows. These RDRs are used to create statistical histograms such as Top TCP Ports.
- Transaction Usage RDRs—Generated for every flow according to user-defined filters. These RDRs contain detailed Layer 7 information for browsing, streaming, and voice flows. They are used for flow-based billing.
- Real-Time Signaling RDRs—Generated to indicate specific network events such as flow start or end. These RDRs are used to signal external systems to allow real-time actions across the network.
- Malicious Traffic RDRs—Generated to indicate that the Cisco SCE platform has detected a traffic anomaly, such as a DDoS attack. These RDRs are used to detect attacks and attackers to mitigate them.

NetFlow

The following information can be exported using the NetFlow protocol

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

Traffic Control

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

Packages

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

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

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

Another scheme is described in the following section:

Virtual Links Mode

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

For more information, see Quota Management.

Unknown Subscriber Traffic

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

Rules

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

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

Calendars

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

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

Time-Based Rules

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

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

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

Related Topics

Global Bandwidth Control , on page 31

Bandwidth Management

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

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

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

Global Bandwidth Control

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

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

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

For each global controller, you can define separate values for the maximum percentage of total available bandwidth separately for each time frame.

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

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

Related Topics

Calendars , on page 31

Quota Management, on page 360

Subscriber Bandwidth Control

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

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

The following parameters specify a BWC:

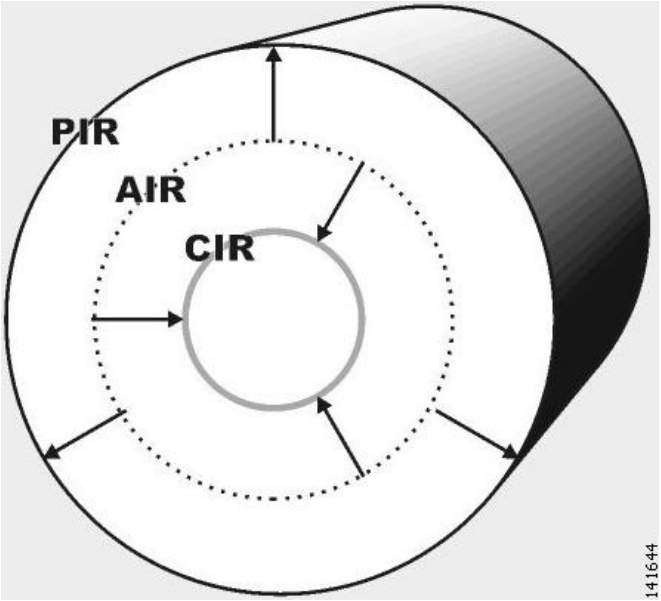
- Committed Information Rate (CIR)—The minimum bandwidth that must be granted to the services that a BWC control.
- Peak Information Rate (PIR)—The maximum bandwidth that can be allocated to the services that a BWC control.
- Global Controller—The global controller to which this BWC links
- Assurance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

The Bandwidth Control Levels figure illustrates the maximum available bandwidth (Admitted Information Rate [AIR]) ranges between the CIR and the PIR. The actual consumed bandwidth is always less than the AIR.

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

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

Figure 7: Bandwidth Control Levels



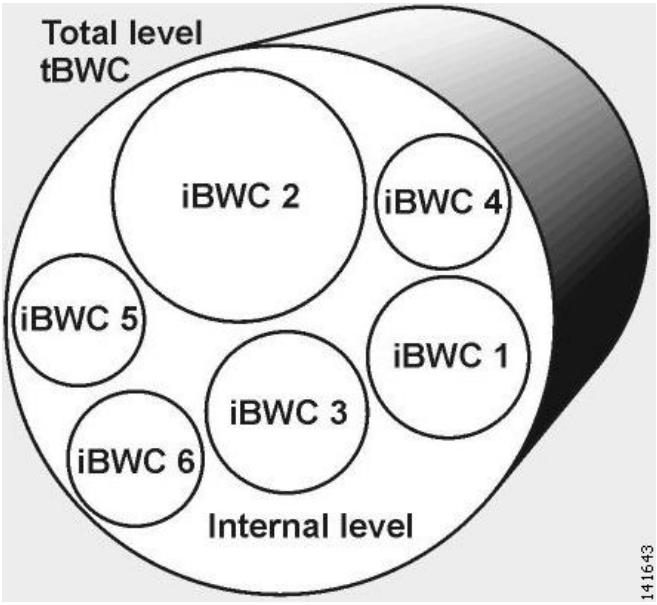
Bandwidth may be thought of in terms of a virtual pipe of adjustable width. The PIR is the maximum allowed width of the virtual pipe. The CIR is the minimum width to which the pipe can contract. The actual pipe width is the AIR. During Network congestion, the system contracts each pipe differently to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

Primary and Internal Bandwidth Control

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

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

Figure 8: Bandwidth Control on Two Levels



You can link iBWCs to traffic in the following way:

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

Quota Management

You can assign subscribers a quota limit on selected services.

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

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

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

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

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

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

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

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

Subscriber Notification

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

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

Service Security

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

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

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

Networks operators can use Cisco SCA BB to:

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

Detecting Malicious Traffic

Cisco SCA BB uses four threat detection mechanisms:

- Anomaly Detection—This set of mechanisms monitors the rate of connections (both successful and unsuccessful) to and from each host IP address. High connection rates or a low ratio between successful and unsuccessful connections indicate malicious activity.
  Anomaly detection characteristics can indicate the following categories of malicious activity:
  - IP sweep—Scanning multiple IP addresses, all on the same port (a behavior typical of worms)
  - Port scan—Scanning all ports at one IP address (a behavior typical of hackers)
  - DoS attack—An attack (on a single IP address) from a single IP address
  - DDoS attack—An attack (on a single IP address) from multiple IP addresses

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

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

Responding to Malicious Traffic

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

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

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

Traffic Filters

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

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

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

A filter rule can also set the DSCP ToS value of the filtered traffic.

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

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

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

DSCP ToS Marking

DSCP ToS marking is used in IP networks to signal the type and priority of a flow between network elements. Typically, those elements that have an insight on how to treat the traffic throughout the network performs the DSCP ToS marking. Such an element can be the element generating traffic—a voice gateway, for example. Cisco SCA BB, being application aware, can, for example, allocate bandwidth resources based on the business model and the specific needs of latency sensitive applications. ToS marking is enabled per direction. You can configure seven DSCP ToS values as an action of the Package rules or for Flow Filter rules. The range is any integer from 0 to 63.

Traffic Forwarding to Value-Added Services Servers

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



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

Service Configurations

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

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

A service configuration consists of:

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

Defining Service Configurations in Practice

In practice, defining service configurations is an iterative process. It is recommended that you use the following sequence of steps:

Procedure

Step 1 Set up the system.

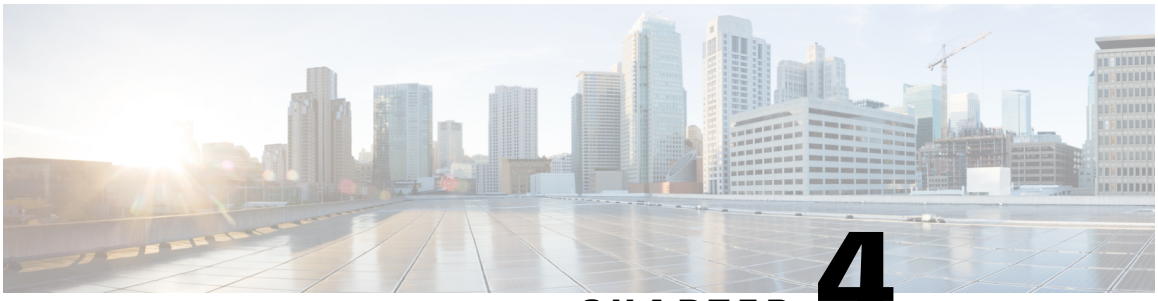
Step 2 Apply the default service configuration.

Step 3 Gather data.

Step 4 Analyze.

Step 5 Do one or both of the following:

- Continue traffic discovery by partitioning the traffic into (additional) services.
- Create rules to limit and prioritize traffic according to services and subscriber packages.



CHAPTER 4

Getting Started with Cisco SCA BB Console

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

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

This section consists of the following sections:

- How to Install Cisco SCA BB , page 39
- How to Upgrade Cisco SCA BB Components, page 44
- Working with Protocol Packs , page 55
- Launching the Cisco SCA BB Console , page 66
- How to Use the Cisco SCA BB Console , page 68
- QuickStart with the Cisco SCA BB Console , page 103

How to Install Cisco SCA BB

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

You install Cisco SCA BB in two stages:

1 Install the Cisco SCA BB front ends:

- The Cisco SCA BB Console
- The Cisco SCA BB Service Configuration Utility, the Cisco SCA BB Signature Configuration Utility, and the Cisco SCA BB Real-Time Monitoring Configuration Utility

2 Install the Cisco SCA BB application components:

- The Cisco SCA BB Service Modeling Language Loadable Image (SLI) and the Cisco SCA BB Service Control Engine (Cisco SCE) applicative management plug-in
- The Cisco SCA BB Subscriber Manager applicative management plug-in (for systems with a Cisco Service Control Subscriber Manager)

If you are upgrading an existing installation of Cisco SCA BB, see the Upgrading the SCE Using the SCE Software Upgrade Wizard, on page 44 section or the Working with Protocol Packs section.

The Cisco SCA BB Installation Package

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

The installation package consists of the following files:

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

Installing Cisco SCA BB Application Components

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

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

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

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

To install these components from the Console, see the Installing PQI Files on Cisco SCE Devices and Introduction to Managing Collection Manager Devices sections.

To install these components from a command line, see the Installing a Cisco SCA BB PQI File on a Cisco SCE Platform section.

Prerequisites

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

Verifying that the SCE Platform is Operational

Procedure

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

Verifying that the SCE Platform is Running an Appropriate Version of the OS

Procedure

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

Step 2 Press Enter .
The response shows the version of the OS running on the SCE platform.

Verifying that the Subscriber Manager is Correctly Installed

Procedure

Step 1 Open a Telnet session to the Subscriber Manager.

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

Step 3 Press Enter .
Displays the operational status of the Cisco Service Control Subscriber Manager.

Verifying that an Appropriate Version of the Subscriber Manager is Running

Procedure

Step 1 Open a Telnet session to the Subscriber Manager.

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

Step 3 Press Enter .

Displays the Subscriber Manager version.

How to Install Cisco SCA BB Front Ends

You should install the following Cisco SCA BB front ends:

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

Cisco SCA BB Hardware Requirements

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

Cisco SCA BB Operating System Requirements

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

Installing the Java Runtime Environment

The Cisco SCA BB Service Configuration Utility, **servconf,** requires access to JRE version 1.6 update 43.

Procedure

Step 1 Verify the version of the JRE installed on the system.
From the command prompt, run **java -version** . The Java version should start with 1.6.

Step 2 (Optional) Configure the JAVA_HOME environment.
If a different version of JRE is also installed on the workstation, configure the JAVA_HOME environment variable in the **servconf** file to point to the JRE 1.6 installation directory.

Example:
JAVA_HOME=C:\Program Files\Java\jre1.6.0_43

Installing the Cisco SCA BB Console

Procedure

Step 1 Navigate to the Console installation file on your local machine, sca-bb-console-4.1.x.exe, and double-click it.
The Welcome page of the Cisco SCA BB Console 4.1.x Setup wizard appears.

Step 2 Click Next .
The Install Location page of the Setup wizard opens.

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

Step 4 Click Next .
The Start Menu Folder page of the Setup wizard opens.

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

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

Step 7 Click Install .
The Installing page of the Setup wizard opens.

Step 8 Wait until the installation is complete.
The Next button is enabled.

Step 9 Click Next .
The Installation Complete page of the Setup wizard opens.

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

Step 11 Click Finish .
The Cisco SCA BB Console 4.1.x Setup wizard closes. The Console is now installed on the machine. A shortcut is added to the Start menu.

Installing the Cisco SCA BB Configuration Utilities

Procedure

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

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

How to Upgrade Cisco SCA BB Components

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

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



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

- When you upgrade old PQB files, some protocol IDs are changed automatically. Messages such as the following may be displayed to indicate the change:
  - Protocol ID of PPLive changed from 81 to 44
  - Protocol ID of BaiBao changed from 80 to 43
- When you upgrade a device with a new SPQI or PQI file, all other devices that are not upgraded may fail.
- New Cisco SCA BB releases do not use the default Dynamic Signature Script (DSS) file (see that it was installed for a previous Cisco SCA BB release).
- If a protocol pack for the new release is available, install it after the product installation is complete. Do *not* install an old protocol pack on top of a new product installation.

Upgrading the SCE Using the SCE Software Upgrade Wizard

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

Procedure

Step 1 Open the Network Navigator.

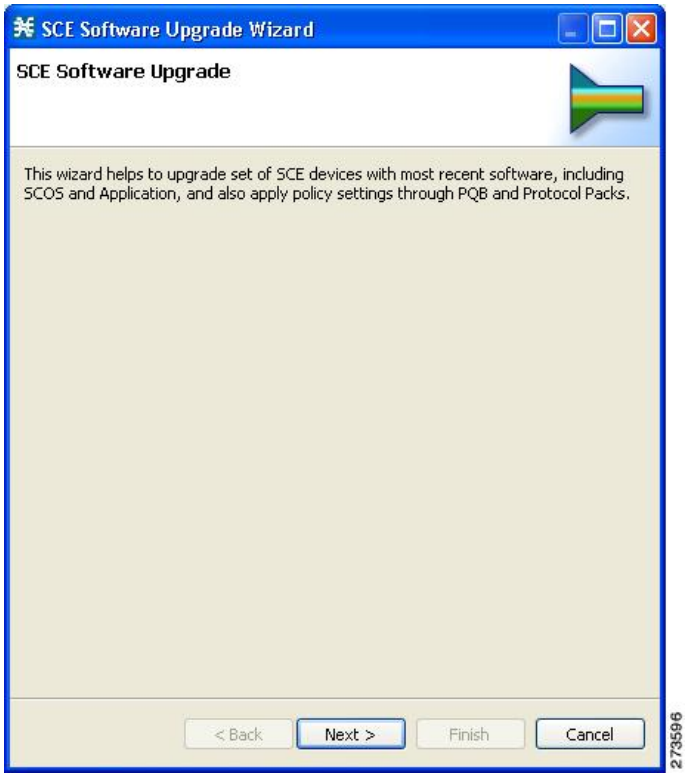
Step 2 Choose one or more devices in the Site Manager tree.

Step 3 Right-click one of the selected devices.

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

The SCE Software Upgrade wizard appears.

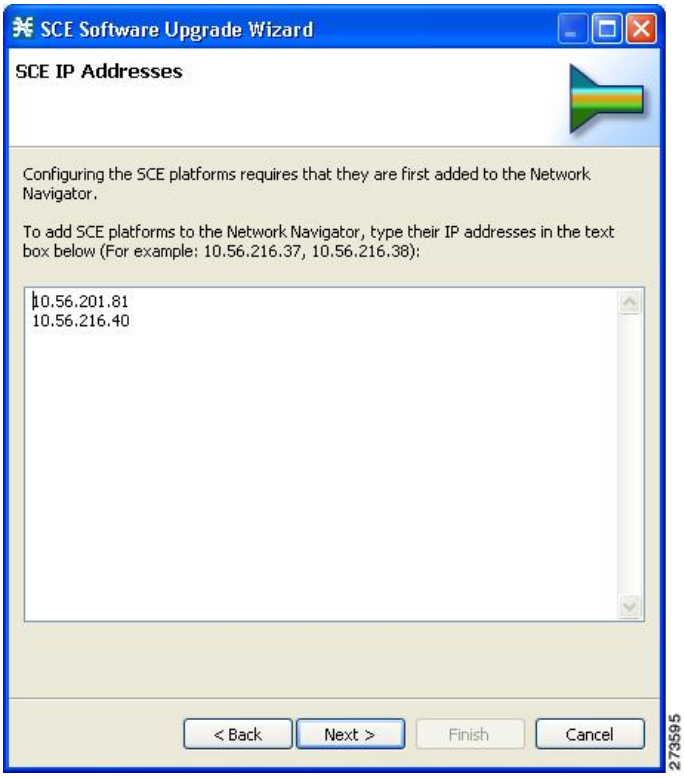
Figure 9: SCE Software Upgrade



Step 5 Click Next .

The SCE IP Addresses page of the SCE Software Upgrade wizard opens.

Figure 10: SCE IP Address

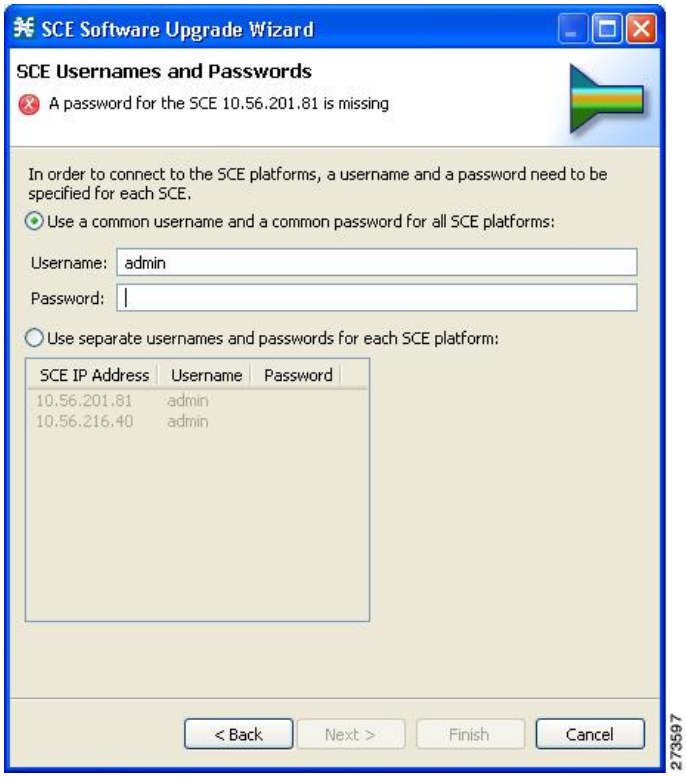


Step 6 (Optional) In the edit box, enter additional IP addresses.

Step 7 Click Next.

The SCE Usernames and Passwords page of the SCE Software Upgrade wizard opens.

Figure 11: SCE Usernames and Passwords



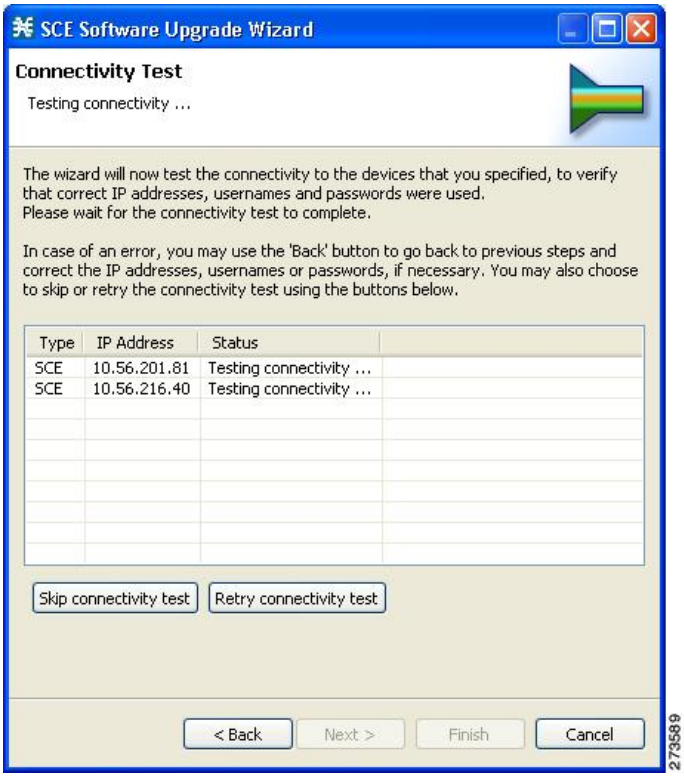
Step 8 Enter the usernames and passwords for the SCE devices.
Do one of the following:

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

Step 9 Click **Next**.

The Connectivity Test page of the SCE Software Upgrade wizard opens.

Figure 12: Connectivity Test



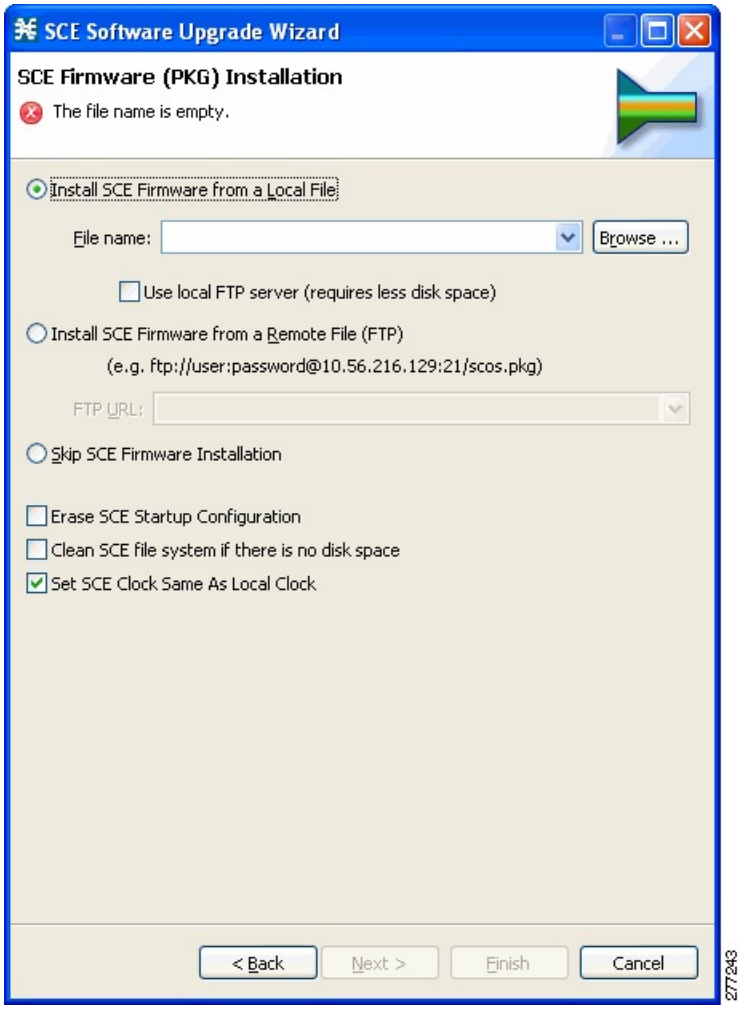
The wizard tests to see that the connections to the defined devices can be made.

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

Step 10 Click **Next**.

The SCE Firmware (PKG) Installation page of the SCE Software Upgrade wizard opens.

Figure 13: SCE Firmware (PKG) Installation



Step 11 Choose the SCE Firmware installation file.

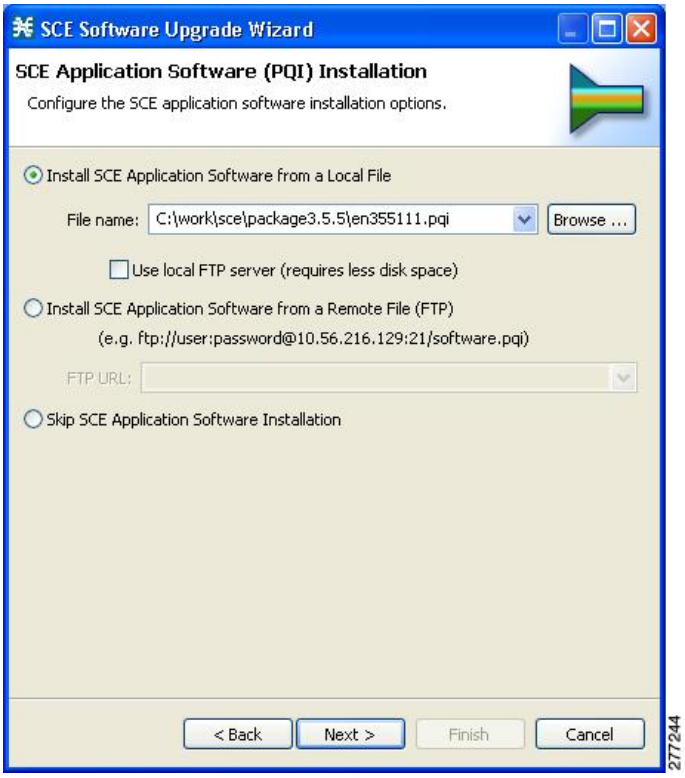
a) To install SCE Firmware from a local file, click **Browse**.
b) Browse to the SCE Firmware installation file that you are installing.
c) Check the Use local FTP server check box to reduce the disk space usage.
d) To download SCE Firmware from a remote site, choose the Install SCE Firmware from a Remote File (FTP) radio button and in the FTP URL field, enter the URL.

Step 12 Click the Skip SCE Firmware Installation radio button.

Step 13 Click Next.

The SCE Application Software (PQI) Installation page of the SCE Software Upgrade wizard opens.

Figure 14: SCE Application Software (PQI) Installation



Step 14 Choose the PQI installation file. Do one of the following steps:

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

b) Browse to the PQI file that you are installing.

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

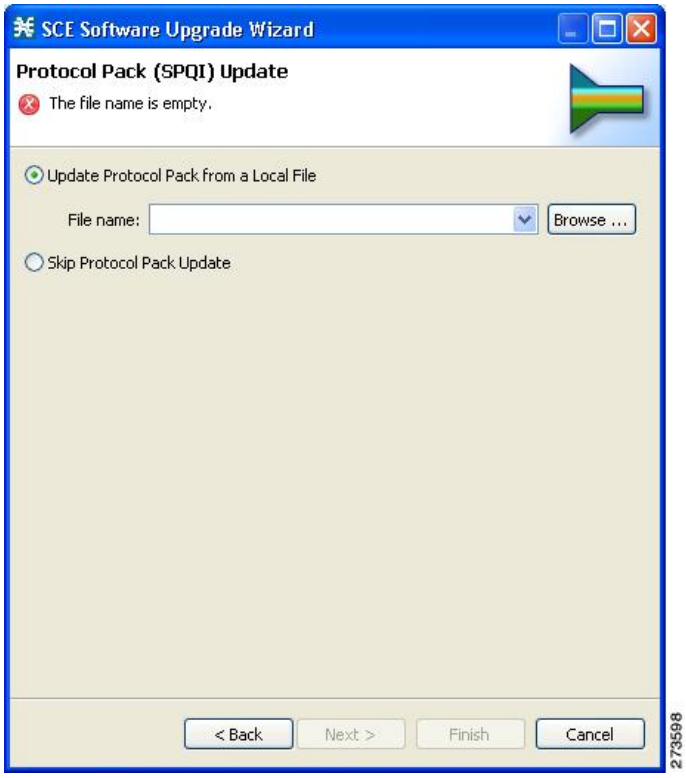
a) To download a PQI file from a remote site, choose the Install SCE Application Software from a Remote File (FTP) radio button and in the FTP URL field, enter the URL.

b) Click the Skip SCE Software Application Installation radio button.

Step 15 Click **Next**.

The Protocol Pack (SPQI) Update page of the SCE Software Upgrade wizard opens.

Figure 15: Protocol Pack (SPQI) Update



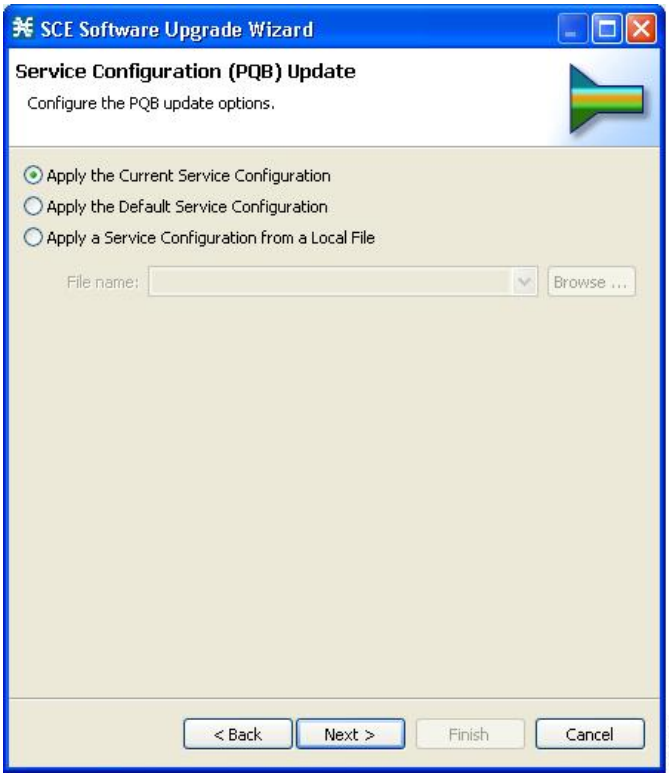
Step 16 Update the protocol pack.
Do one of the following:

- To update the SPQI file from a local file, click Browse. A Select file dialog box appears. Browse to the SPQI file that you are updating.
- Click the **Skip Protocol Pack Update** radio button.

Step 17 Click **Next** .

The Service Configuration (PQB) Update page of the SCE Software Upgrade wizard opens.

Figure 16: Service Configuration (PQB) Update



Step 18 Choose one of the PQB update options.

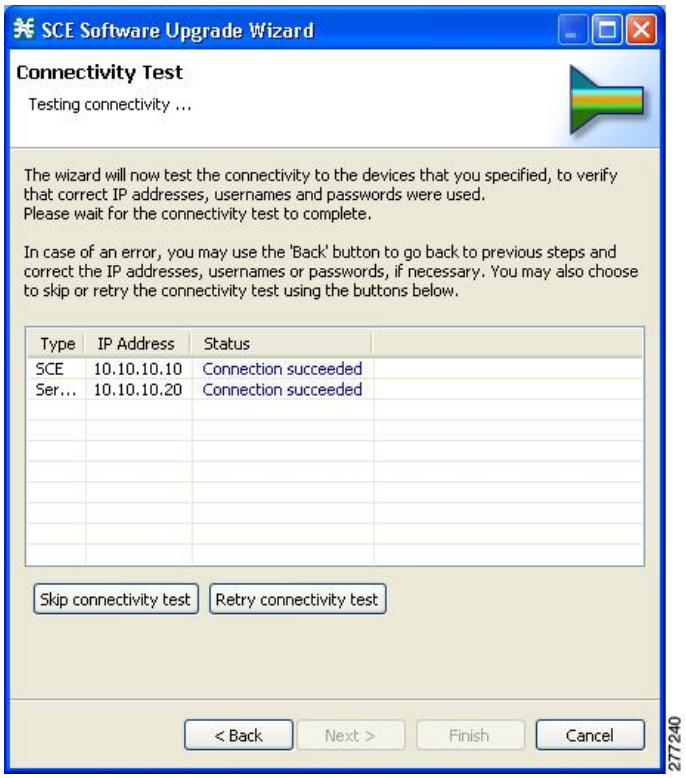
- Apply the Current Service Configuration—Keep the existing service configuration.
- Apply the Default Service Configuration—Apply the default service configuration delivered with the product.
- Apply the Service Configuration from a Local File—Apply a service configuration from a local file.

Step 19 If you selected the Apply the Service Configuration from a Local File radio button, click **Browse** .
A Select file dialog box appears. Browse to the file containing the service configuration.

Step 20 Click **Next**.
The Connectivity Test window of the SCE Software Upgrade wizard opens. The connectivity test verifies the connections to the defined devices.

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

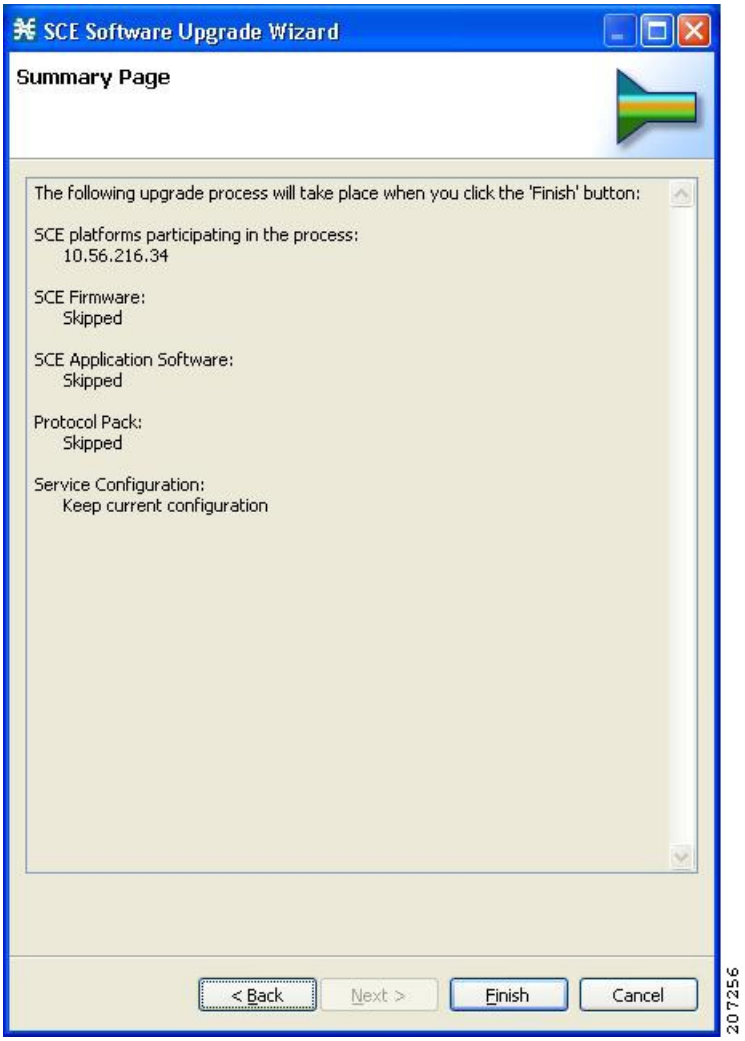
Figure 17: Connectivity Test



Step 21 Click **Next** .

The Confirmation page of the SCE Software Upgrade wizard opens.

Figure 18: Summary Page

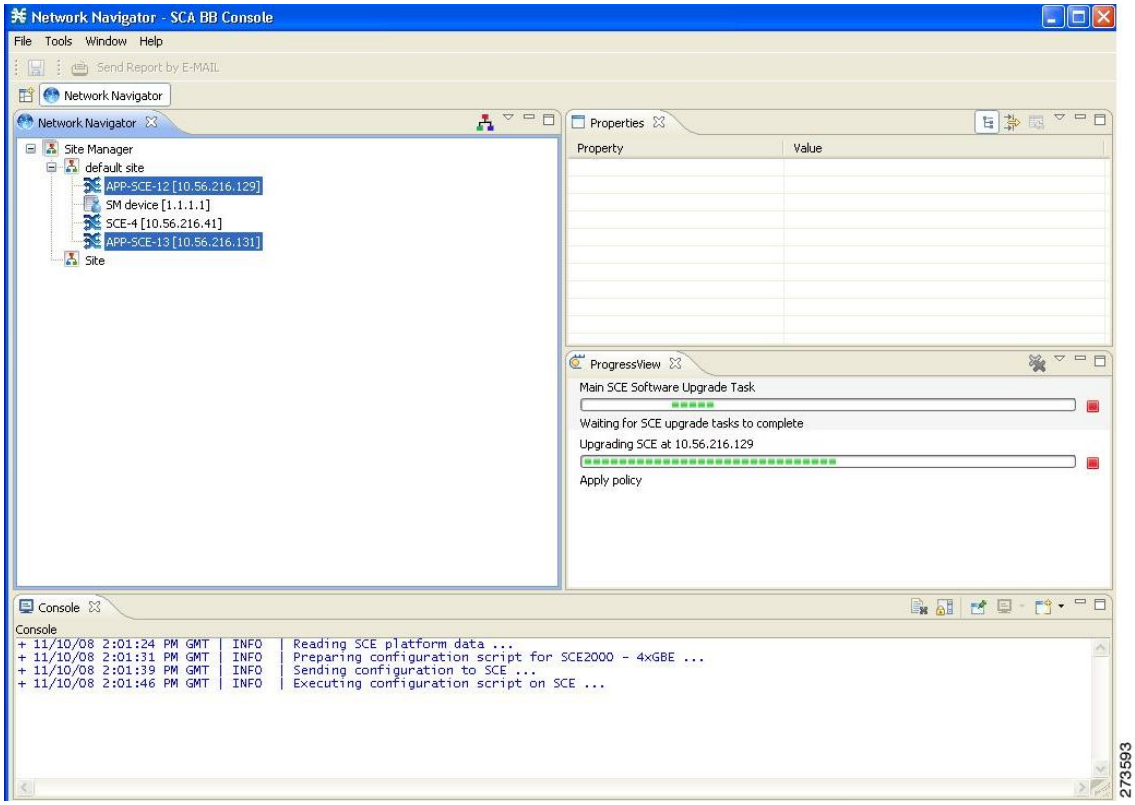


The actions that the wizard is about to take are listed on the page.

Step 22 Click **Finish**.

You can view the progress in the Progress view.

Figure 19: Progress



Working with Protocol Packs

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

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

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

Protocol Packs

Periodically, Cisco publishes protocol packs containing new and improved protocol signatures for Cisco SCA BB. A typical protocol pack is a file containing signatures for detecting network worms, popular peer-to-peer

applications, and other relevant protocols. When loaded into SCE platforms, these signatures improve Cisco SCA BB classification abilities.

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

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

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

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

Installing Protocol Packs

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

- The Cisco SCA BB Service Configuration Utility (see the The Cisco SCA BB Service Configuration Utility section)
- The Network Navigator tool (see the Installing a Protocol Pack on a Single Cisco SCE Platform section)

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

The tool or utility performs the following steps: Retrieves the current service configuration from the SCE platform and (optionally) stores a backup copy in a folder that you specify.

Note Cisco SCE does not support direct downgrade of higher PP versions to a lower PP version. While downgrading the protocol pack from a higher version to a lower version, the Cisco SCA BB console displays an error message and prevents you from applying the policy on the Cisco SCE.

Procedure

Step 1 Retrieves the current service configuration from the SCE platform and (optionally) stores a backup copy in a folder that you specify.

Step 2 Imports the signatures that are in the DSS or SPQI file into the service configuration. This action overwrites any DSS that was previously imported into the service configuration.

Step 3 For each new signature that includes a Buddy Protocol attribute (an attribute that points to an existing protocol) (see DSS Buddy Protocol section)—Adds the new signature to all services that include the buddy protocol.

Step 4 If the protocol pack is an SPQI file—Replaces the SCE application. This action causes a short (up to one minute) downtime in SCE platform service.

Step 5 Applies the new service configuration to the SCE platform.
If the protocol pack is an SPQI file and the hitless upgrade option is enabled, you can monitor the progress of the upgrade using the hitless upgrade CLI commands (see the Hitless Upgrade CLI Commands section.)

How to Install the Service Hierarchy Tree

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

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

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

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

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

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

Note Common SCABB console is going to be used in SCE 8000 platform releases.

SCE 8000 platform level service tree will be maintained if we open 4.1.x, 5.1.x or any earlier release PQB file in 5.2.0 SCABB console.

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

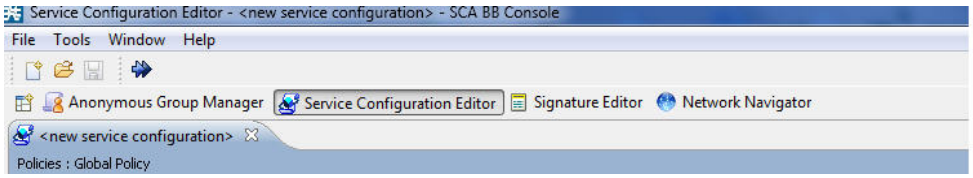
Viewing and Installing the Service Hierarchy Tree

Procedure

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

Step 2 From the toolbar, select Service Configuration Editor.

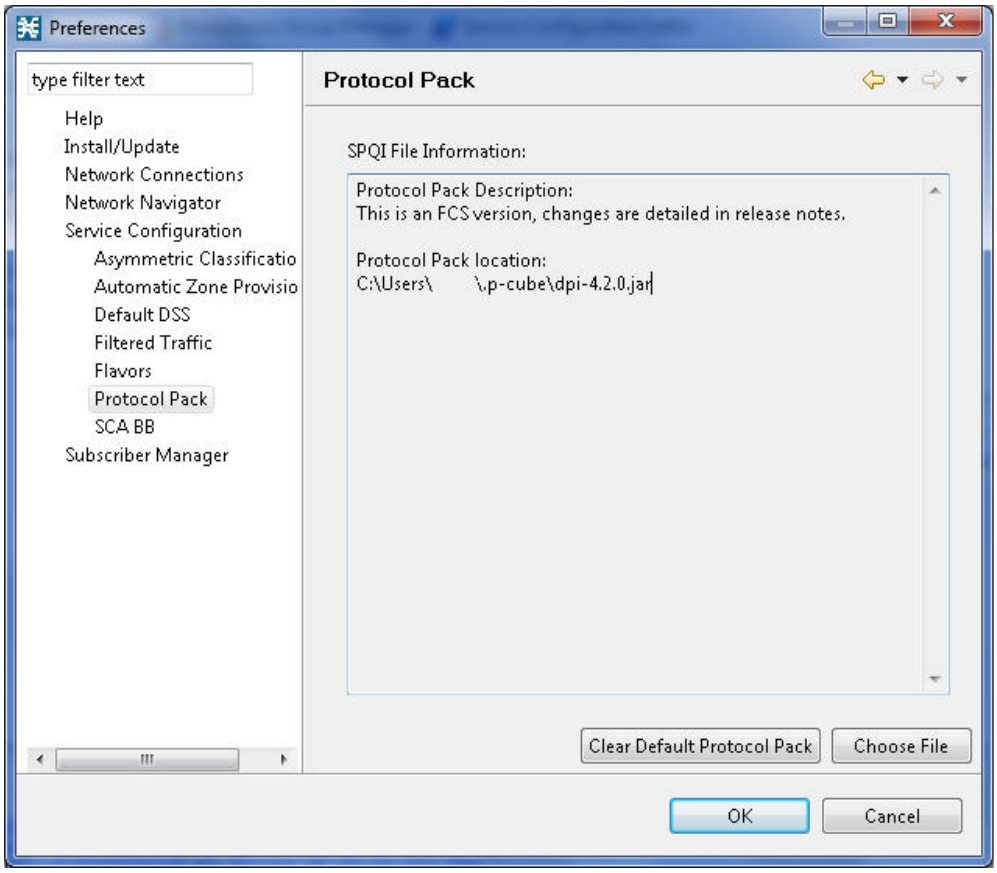
Figure 20: Service Configuration Editor - Preferences



Step 3 Select Windows > Preferences and then select Service Configuration.

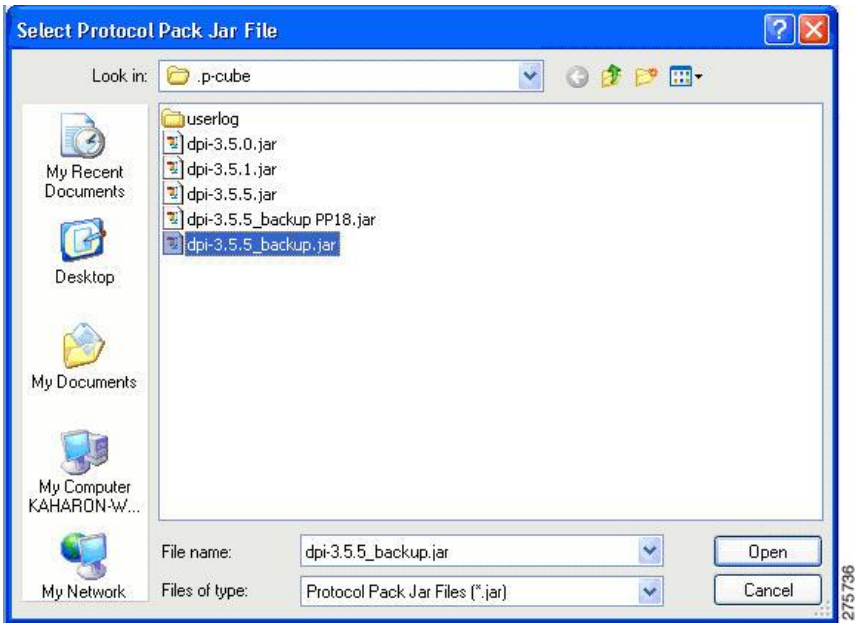
Step 4 Select Protocol Pack from the Service Configuration tree. The upper window provides information related to service hierarchy tree related to the GUI.

Figure 21: Preferences (Filtered)



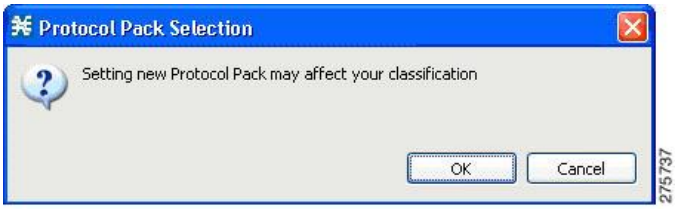
Step 5 To install a new service hierarchy tree, click the Choose File button and select either a jar file or an SPQI file.

Figure 22: Select Protocol Pack



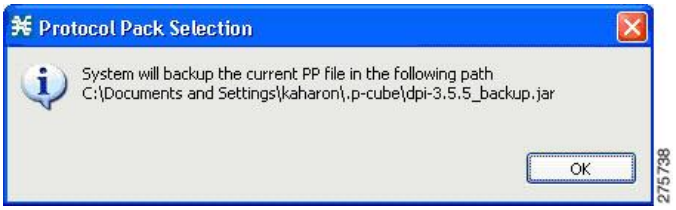
Step 6 Click **Open**, and approve the warning message by clicking **OK** .

Figure 23: Protocol Pack Selection Warning Message



Step 7 To back up the current protocol pack and install the new service hierarchy tree, approve the backup message by clicking **OK**.

Figure 24: Protocol Pack Selection Backup Message

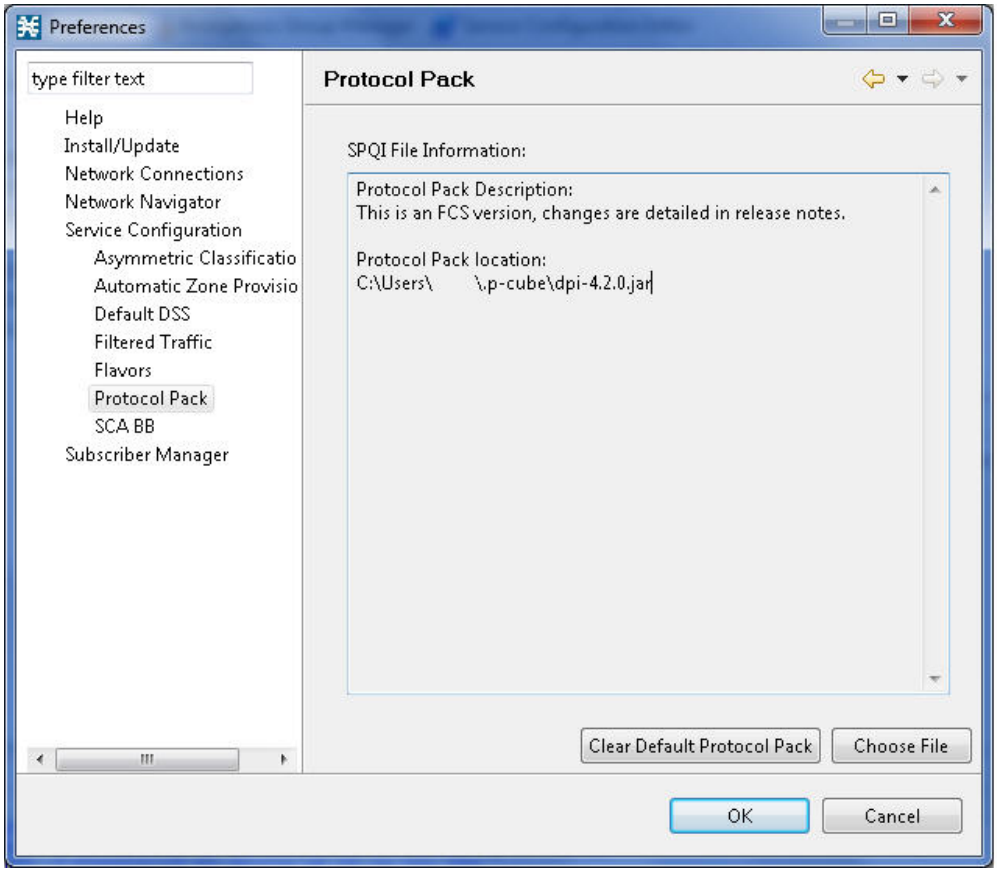


Removing the Service Hierarchy Tree

Procedure

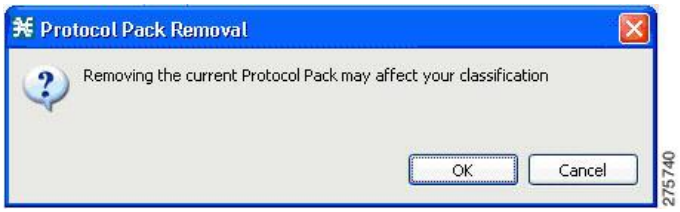
Step 1 To remove the service hierarchy tree and to return to the default configuration, click the Clear Default Protocol Pack button in the Preferences window.

Figure 25: Preferences (Filtered)



Step 2 Accept the operation by clicking OK on the Protocol Pack Removal message screen.

Figure 26: Protocol Pack Removal Message



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

Verifying Version Compatibility for Protocol Packs

A protocol pack is compatible only with specific versions of the SCE application. When working with protocol packs, verify that the protocol pack version matches the SCE application version. For example, only use a protocol pack for 4.0.0 on SCE application version 4.0.0.

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

Procedure

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

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

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

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

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

The application version should match that of the protocol pack.

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

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

Verifying the Installation of a Protocol Pack

Procedure

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

Step 2 Press Enter .
The response shows the version of the OS running on the SCE platform. This response includes information about the installed protocol pack version.

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

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

Causes for Protocol Pack Installation Failure and Remedies

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

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

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

Hitless Upgrade of the SLI

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

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



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

After the new application is loaded on the SCE platform:

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

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

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

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

These criteria are configurable by CLI commands.

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

Hitless Upgrade CLI Commands

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

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

replace completion time <*minutes*>

no replace completion time

default replace completion time

replace completion num-flows <*num*>

no replace completion num-flows

default replace completion num-flows

These commands are line interface configuration commands. To run these commands you must enter line interface configuration mode and see the SCE(config if)# prompt displayed. For details on interface configuration mode, see Entering Line Interface Configuration Mode section.

The following two CLI commands are EXEC mode commands.

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

show applications slot <*num*> **replace**

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

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

Description of Hitless Upgrade CLI Commands

Table 4: Hitless Upgrade CLI Commands

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

Command	Description
show applications slot <*num*> **replace**	Shows the current hitless upgrade state: • Current replace stage • Current completion criteria • Current completion status (elapsed time and number of flows on each traffic processor) • Whether this task is an upgrade or a downgrade • Values for spare memory
application slot <*num*> **replace force completion**	Forces the current hitless upgrade process to complete (killing all old flows).

Entering Line Interface Configuration Mode

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

Procedure

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

Step 2 Press Enter .
The SCE(config)# prompt appears.

Step 3 Type **interface LineCard 0** .

Step 4 Press Enter .
The SCE(config if)# prompt appears.

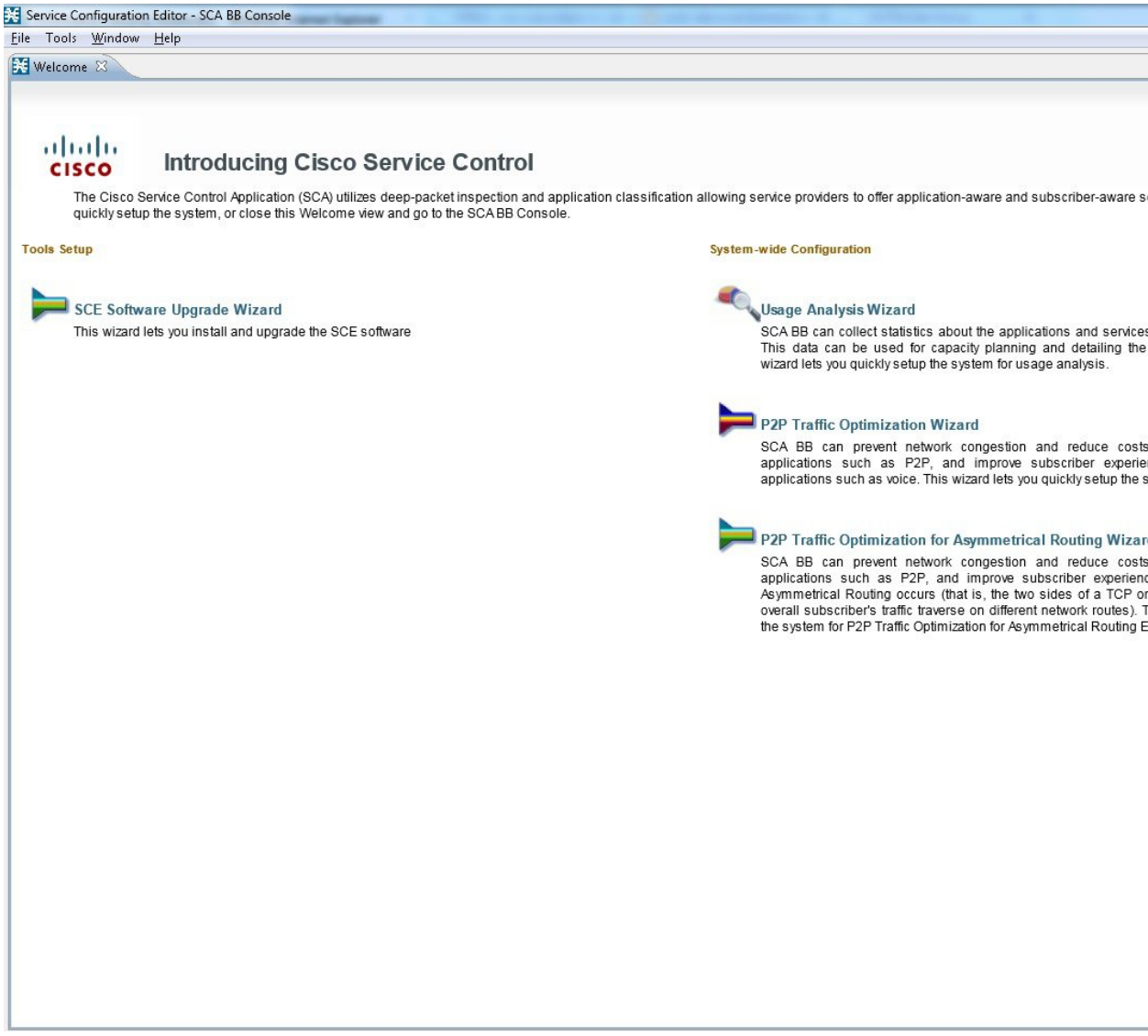
Launching the Cisco SCA BB Console

Procedure

Step 1 Choose Start > All Programs > Cisco SCA > SCA BB Console > 5.2.xSCA BB Console 5.2.x.

The Cisco SCA BB Console splash screen appears. After the Console has loaded, the main window of the Console appears. The first time that you launch the Console, the Welcome view is open in the main window.

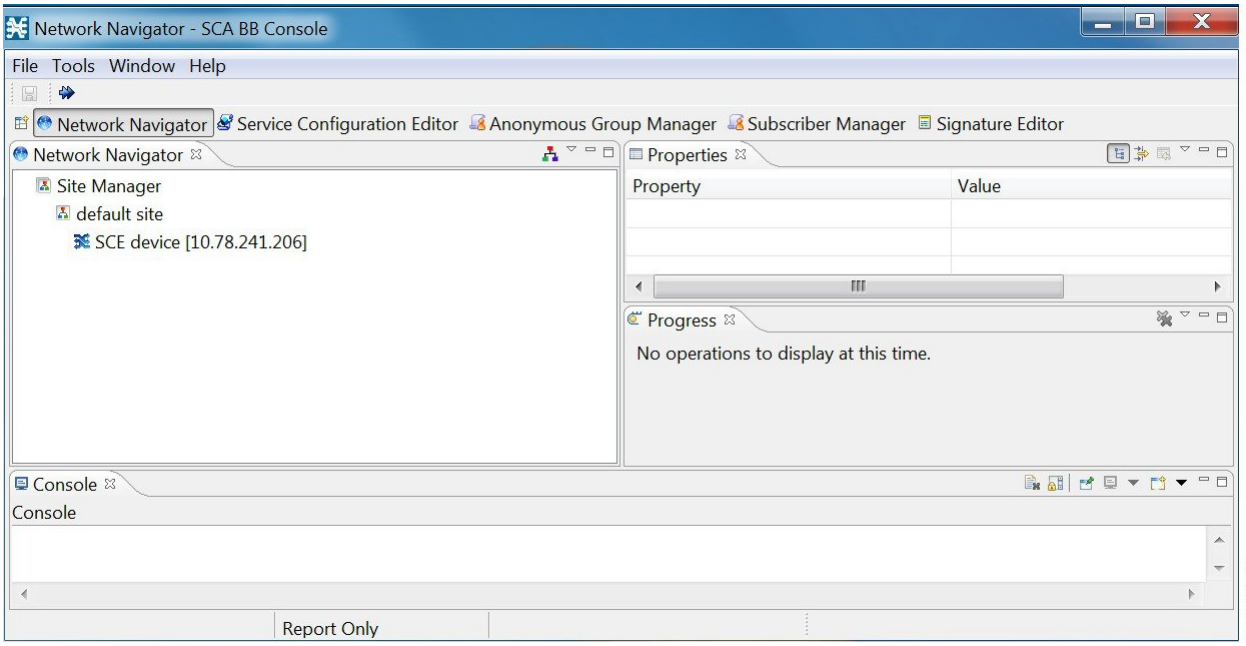
Figure 27: Welcome - Introducing Cisco Service Control



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

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

Figure 28: Network Navigator



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

How to Use the Cisco SCA BB Console

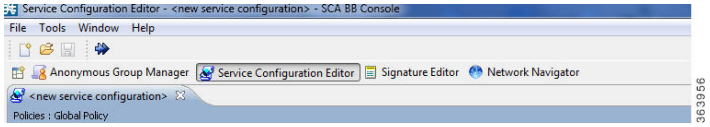
The Console is the front end of Cisco SCA BB. You use it to configure the services that the SP offers to you.

The Console consists of the following tools:

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

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

Figure 29: Menu Bar and Toolbar of the Console GUI



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

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

- Configuration Wizards
- The Network Navigator Tool
- The Service Configuration Editor Tool
- The Signature Editor Tool
- The Subscriber Manager GUI Tool
- The Anonymous Group Manager Tool
- The Reporter Tool
- Online Help

Cisco SCA BB Configuration Wizards

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

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

Asymmetric Routing

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

Anonymous Subscriber Mode

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

Using the Usage Analysis Wizard

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



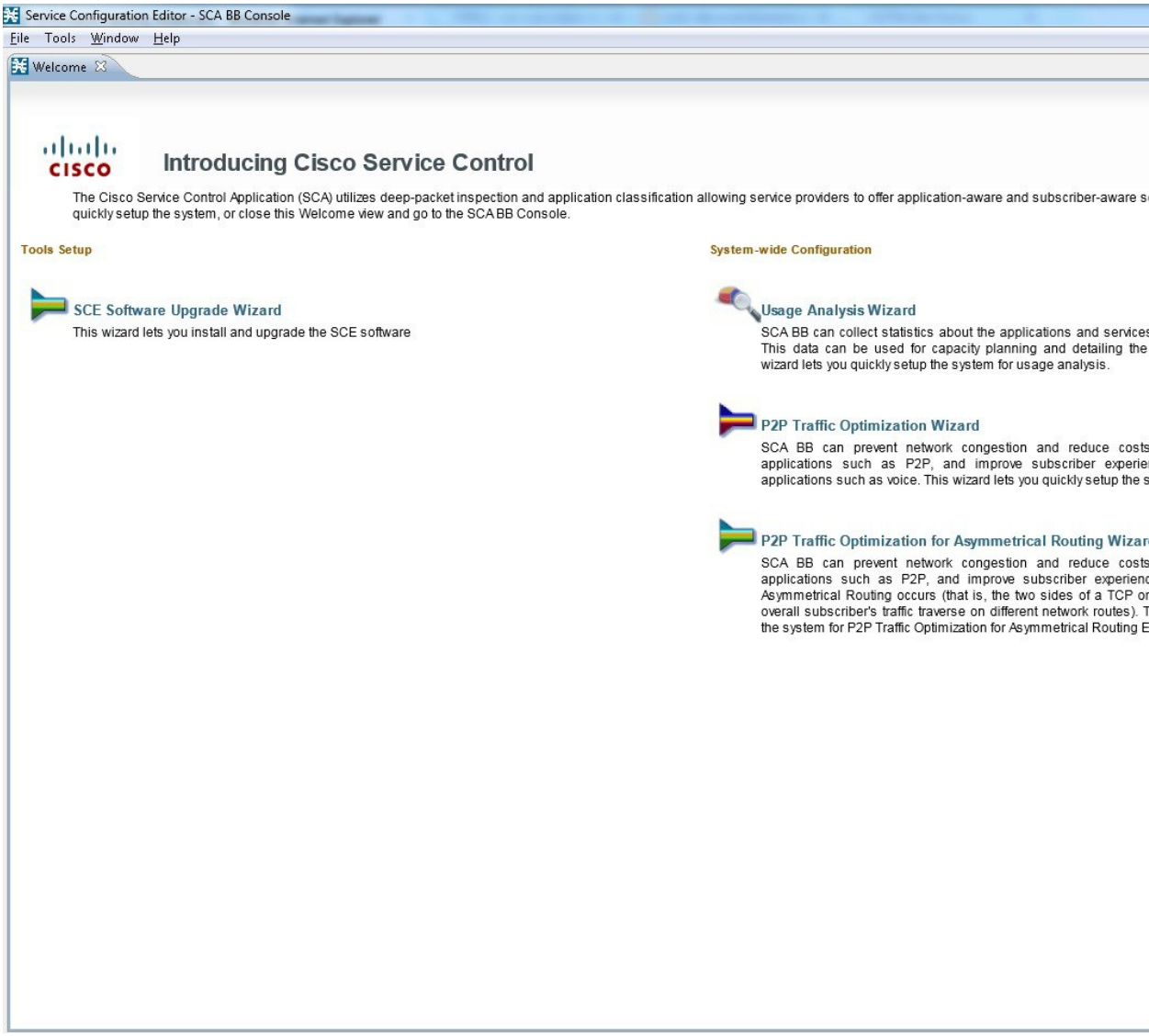
Note If they do not exist, devices defined in the wizard are added to the default site in the Site Manager tree.

Procedure

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

The Welcome view opens.

Figure 30: Welcome - Introducing Cisco Service Control

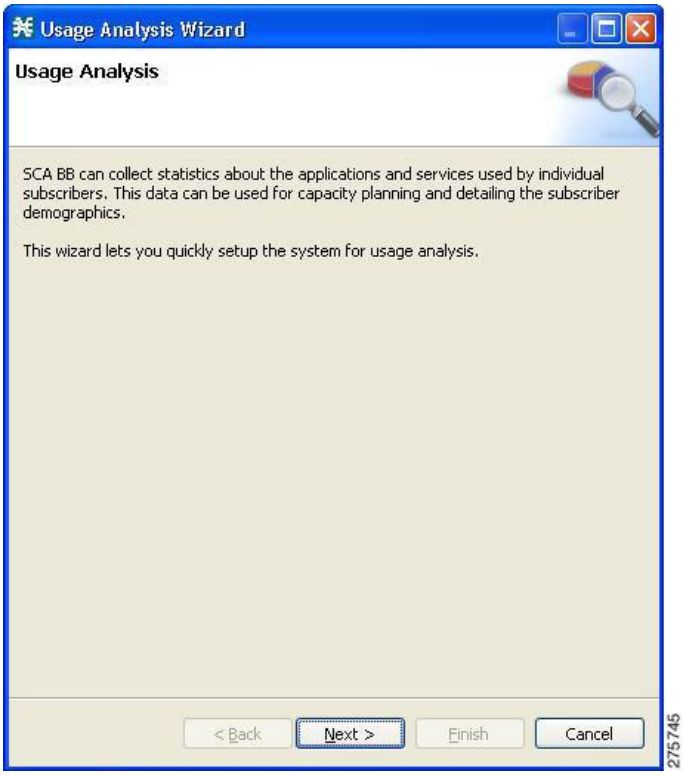


Step 2 Click **Usage Analysis Wizard**.

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

The Welcome page of the Usage Analysis wizard appears.

Figure 31: Usage Analysis

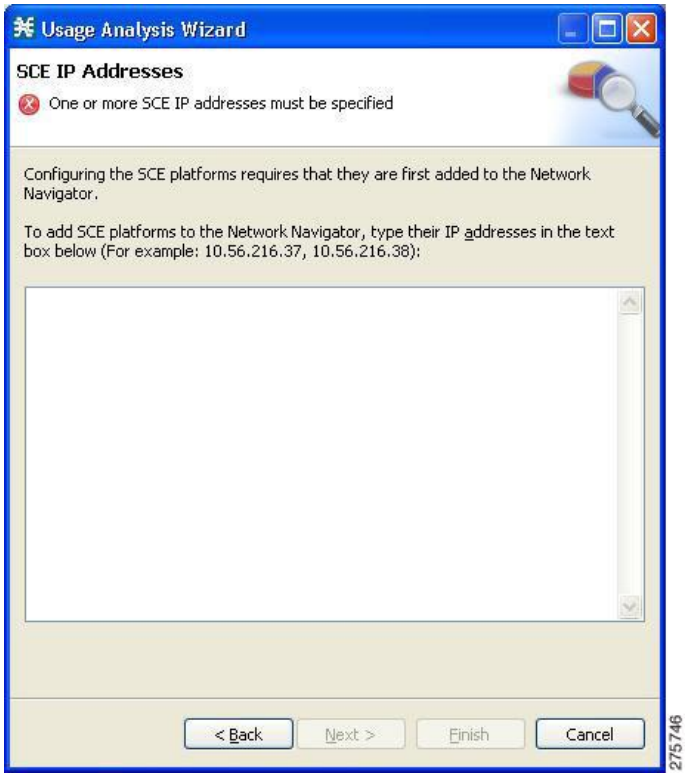


1. Select one or more devices in the Site Manager tree.
2. Right-click one of the selected devices.
3. From the popup menu that appears, select **Configuration Wizards > Usage Analysis Configuration**.
4. You can set only one CM and one Reporter database in the wizard. If you select more than one CM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

Step 3 Click **Next**.

The SCE IP Addresses page of the Usage Analysis wizard opens.

Figure 32: SCE IP Addresses



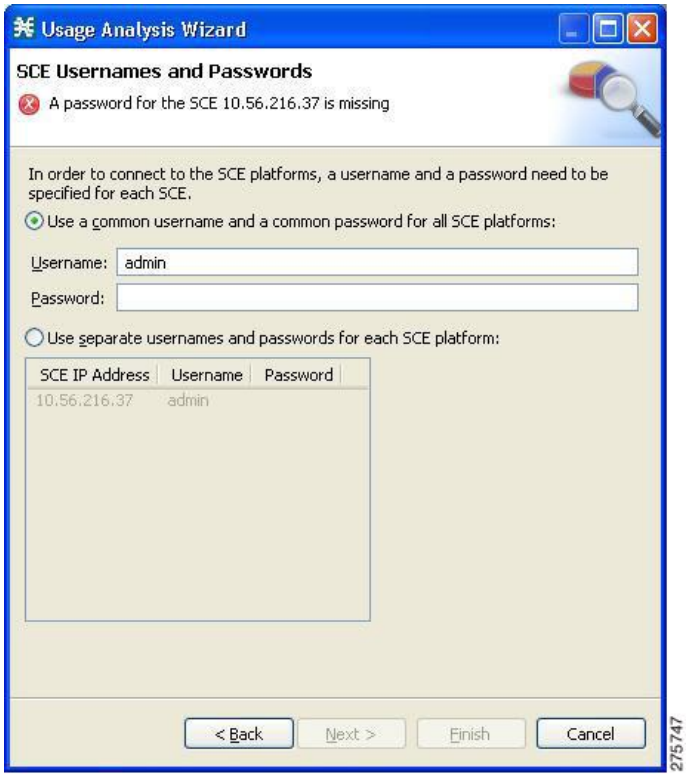
Step 4 In the edit box, enter the IP addresses of the SCE devices that should be added to the model.
If you started from the Network Navigator, the IP addresses of the SCE devices that you selected are displayed in the edit box. You can add additional addresses.

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

Step 5 Click **Next**.

The SCE Usernames and Passwords page of the Usage Analysis wizard opens.

Figure 33: SCE Usernames and Passwords



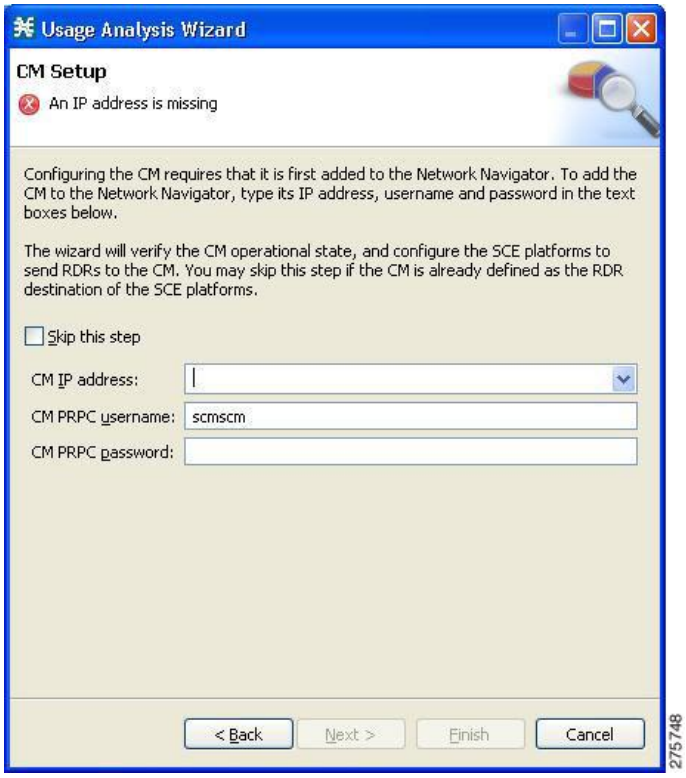
Step 6 Enter the usernames and passwords for the SCE devices.
Do one of the following:

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

Step 7 Click **Next**.

The CM Setup page of the Usage Analysis wizard opens.

Figure 34: CM Setup



Step 8 Define the SCSM Collection Manager (CM) to use with this configuration.
Do one of the following:

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

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

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

Step 9 Click **Next**.

The Reporter Setup page of the Usage Analysis wizard opens.

Figure 35: Reporter Setup



Step 10 Define the database to which the Reporter tool should connect.
Do one of the following:

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

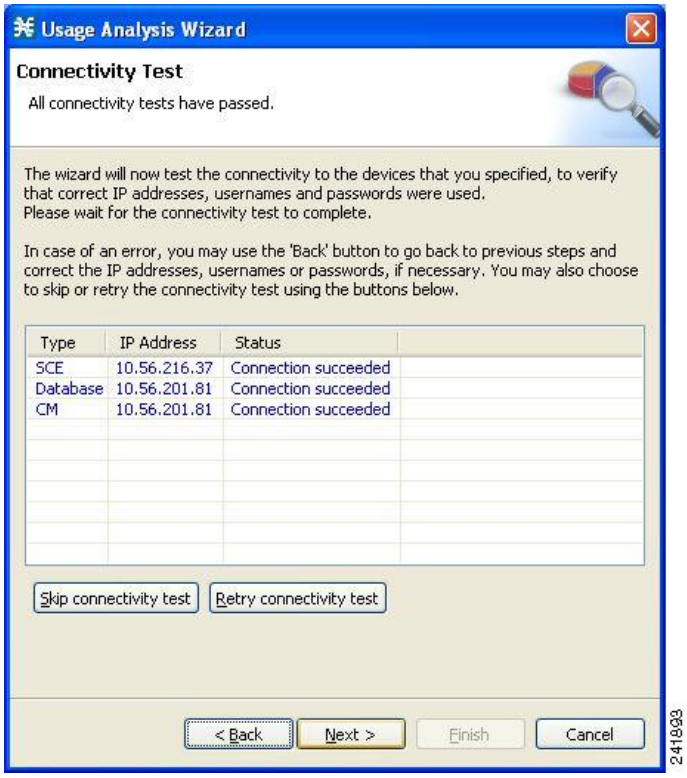
If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.

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

Step 11 Click **Next**.

The Connectivity Test page of the Usage Analysis wizard opens.

Figure 36: Connectivity Test



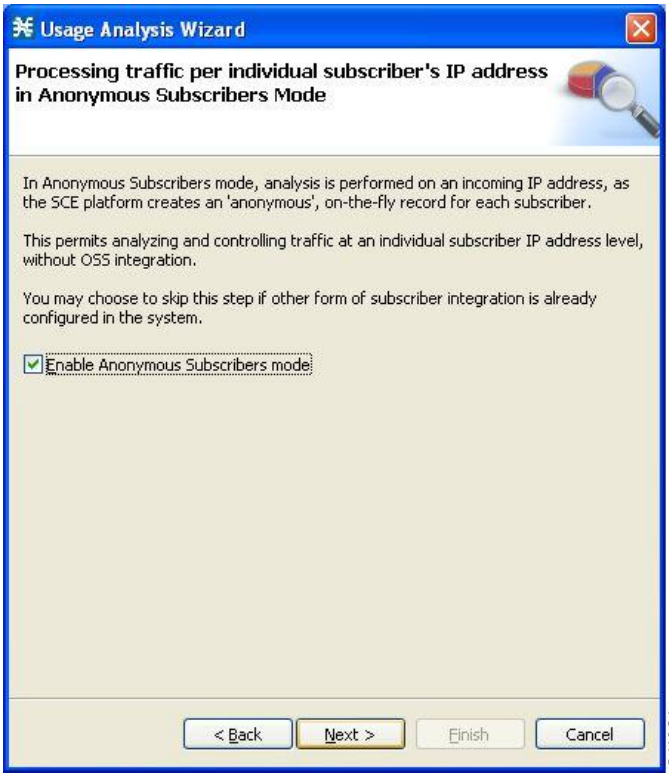
The wizard tests to see that the connections to the defined devices can be made.

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

Step 12 Click **Next**.

The Anonymous Subscribers page of the Usage Analysis wizard opens.

Figure 37: Anonymous Subscribers

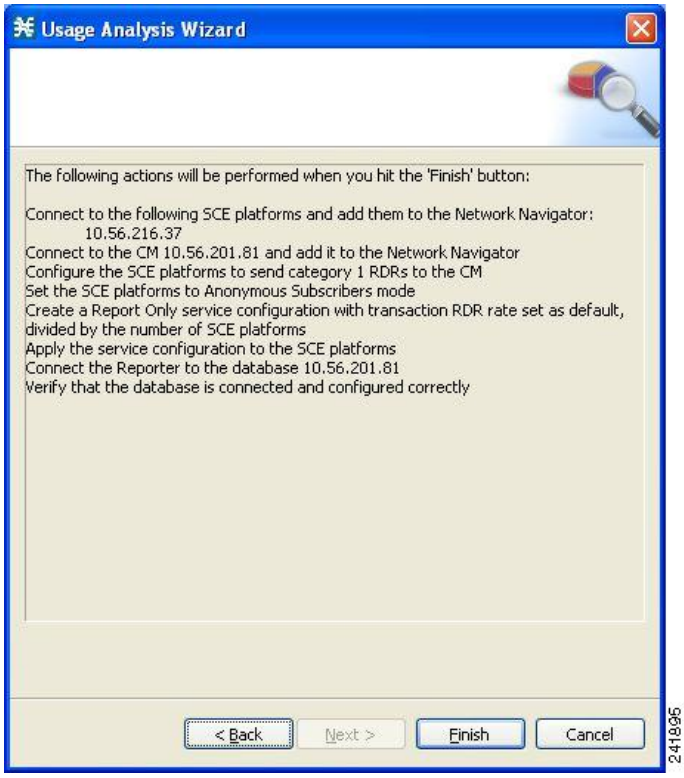


Step 13 To disable anonymous subscriber mode, uncheck the **Enable Anonymous Subscribers mode** check box.

Step 14 Click **Next**.

The Confirmation page of the Usage Analysis wizard opens .

Figure 38: Confirmation

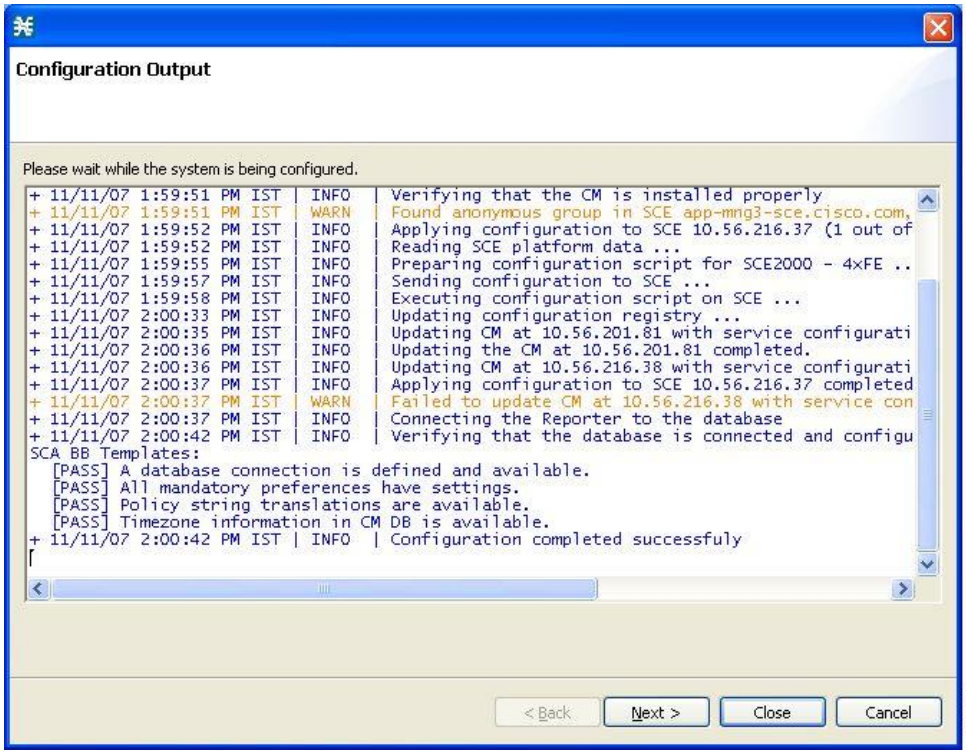


The actions that the wizard is about to take are listed on the page.

Step 15 Click **Finish**.

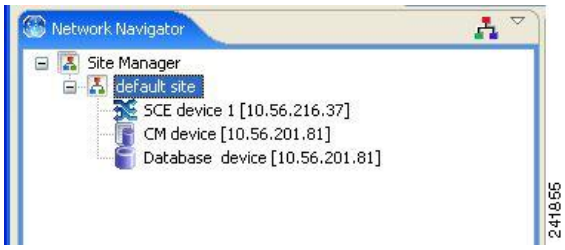
The Configuration Output page of the Usage Analysis wizard opens.

Figure 39: Configuration Output



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

Figure 40: Site Manager Tree



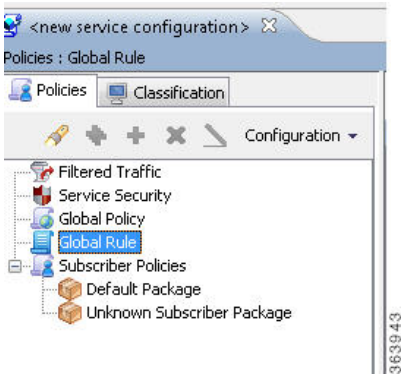
The wizard attempts to connect to all devices that you defined. The operation fails if:

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

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

A new service configuration named Usage Analysis is created, and opens in the Service Configuration Editor.

Figure 41: Service Configuration Editor



The service configuration has the following characteristics:

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

The service configuration is applied to the SCE devices.

If you defined a database in Step 10:

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

Step 16 If you did not define a database in Step 10, click **Close**.
The Usage Analysis wizard closes.

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

Using the P2P Traffic Optimization Wizards

There are two wizards for optimizing P2P traffic:

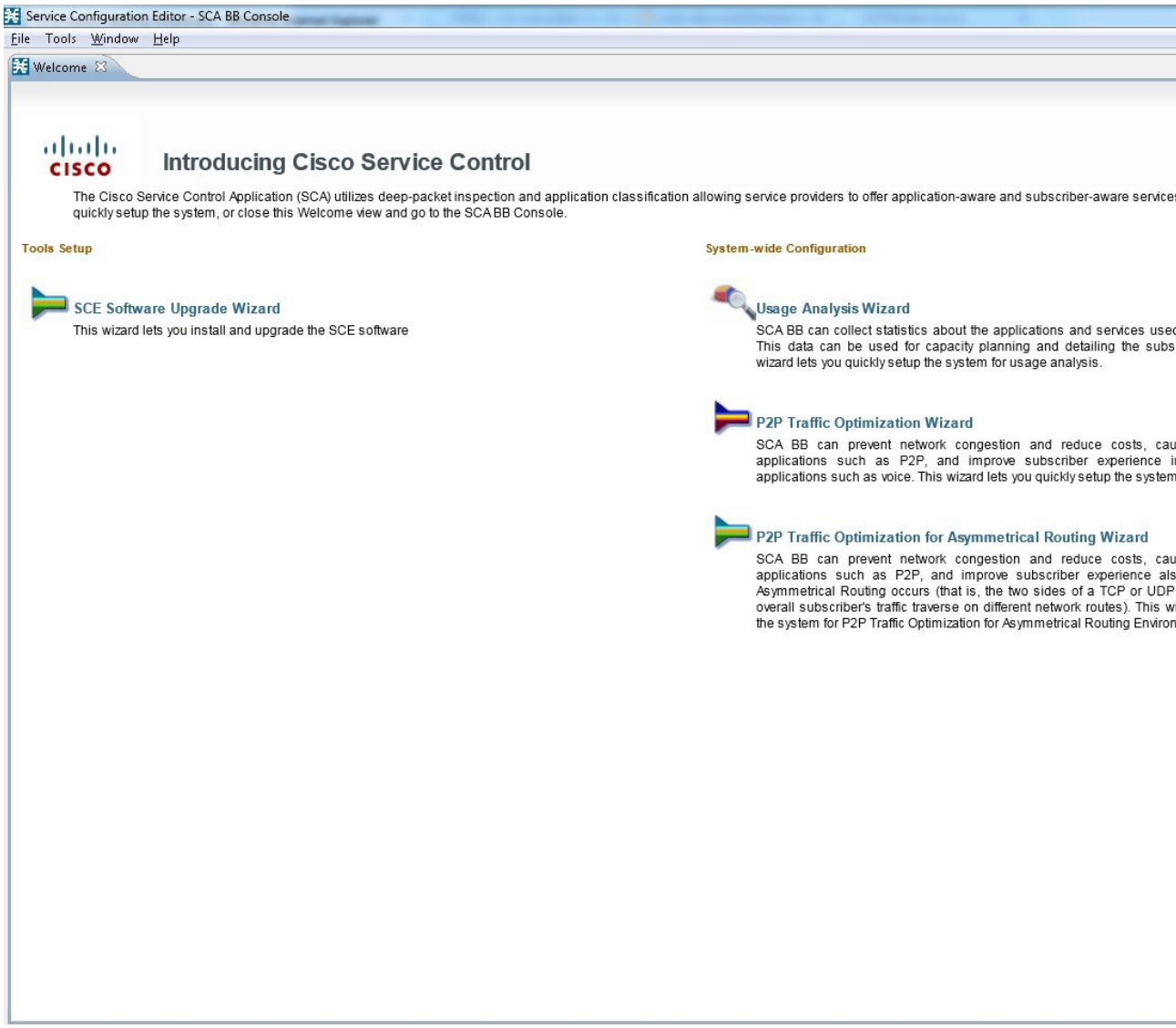
- The P2P Traffic Optimization wizard allows you to create a simple model of devices, connect to them, and limit P2P traffic to a specified percentage of total available bandwidth.
- The P2P Traffic Optimization at a Peering Point wizard allows you to create a simple model of devices, connect to them,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

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

Procedure

Step 1 From the Console main menu, choose Help > Welcome .
The Welcome view opens.

Figure 42: Welcome - Introducing Cisco Service Control



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

The Welcome page of the selected wizard appears.

Figure 43: P2P Traffic Optimization

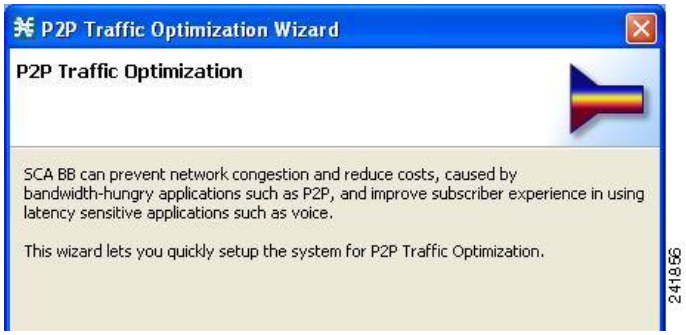
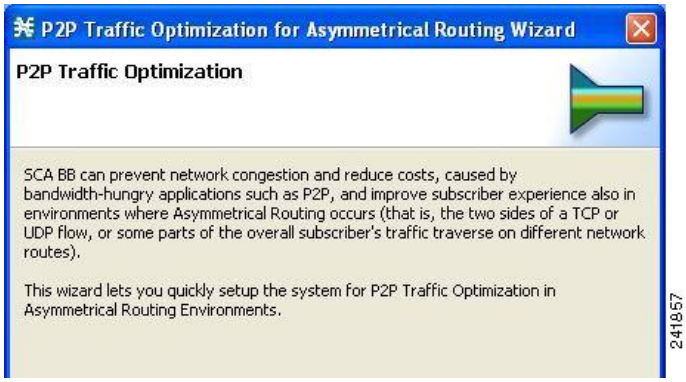


Figure 44: P2P Traffic Optimization for Asymmetrical Routing



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

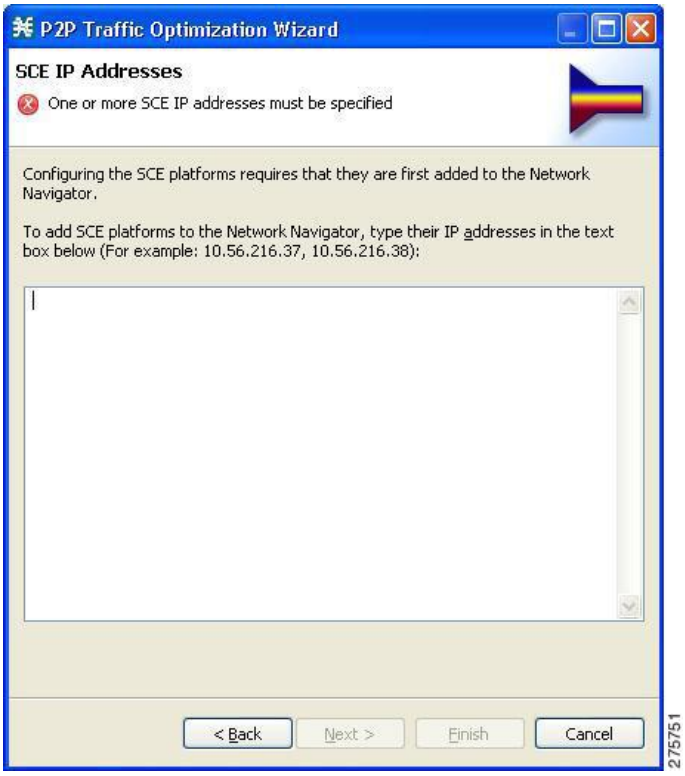
1. Select one or more devices in the Site Manager tree.
2. Right-click one of the selected devices.
3. From the popup menu that appears, choose Configuration Wizards > P2P Traffic Optimization Wizard or Configuration Wizards > P2P Traffic Optimization for Asymmetrical Routing Wizard .

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

Step 3 Click Next .

The SCE IP Addresses page of the P2P Traffic Optimization wizard opens

Figure 45: SCE IP Addresses



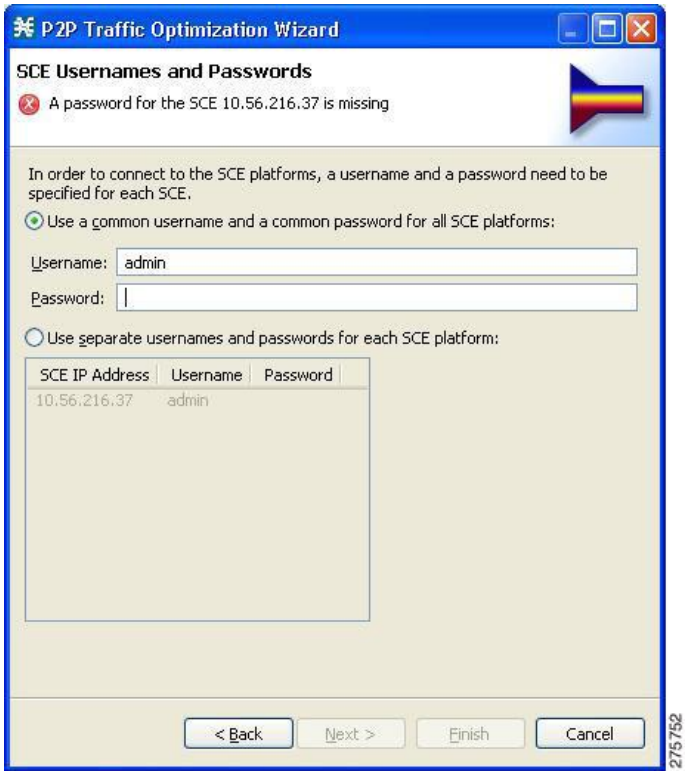
Step 4 In the edit box, enter the IP addresses of the SCE devices that should be added to the model.
If you started from the Network Navigator, the IP addresses of the SCE devices that you selected are displayed in the edit box. You can add additional addresses.

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

Step 5 Click Next .

The SCE Usernames and Passwords page of the P2P Traffic Optimization wizard opens.

Figure 46: SCE Usernames and Passwords



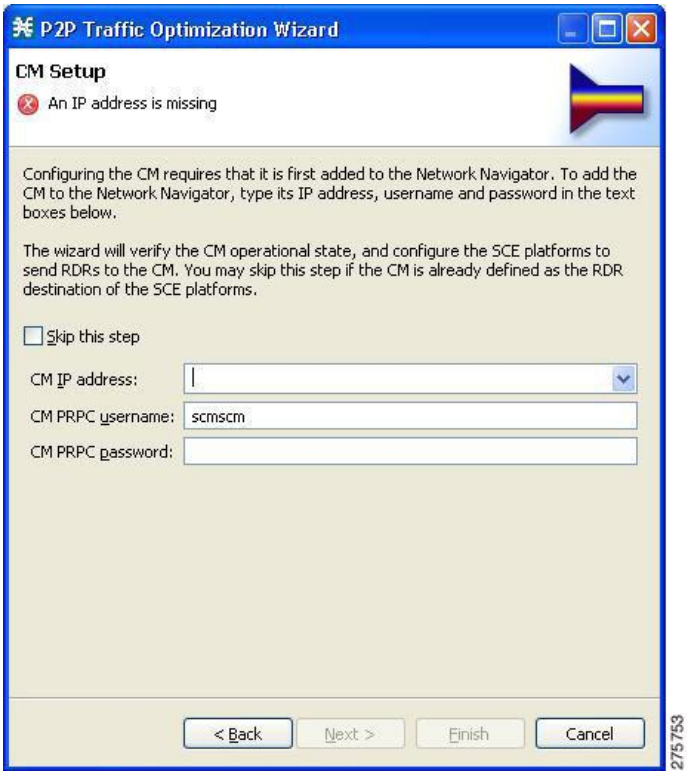
Step 6 Enter the usernames and passwords for the SCE devices.
Do one of the following:

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

Step 7 Click Next .

The CM Setup page of the P2P Traffic Optimization wizard opens.

Figure 47: CM Setup



Step 8 Define the Cisco Service Control Collection Manager (CM) to use with this configuration.
Do one of the following:

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

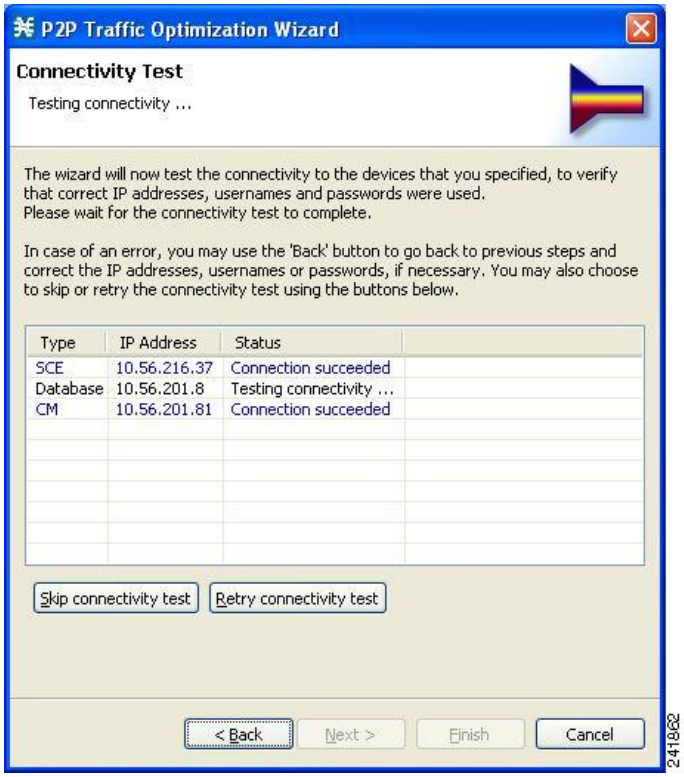
If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.

- Check the Skip this step check box.

Step 9 Click **Next**.

The Connectivity Test page of the P2P Traffic Optimization wizard opens. The wizard tests to see that the connections to the defined devices can be made.

Figure 48: Connectivity Test

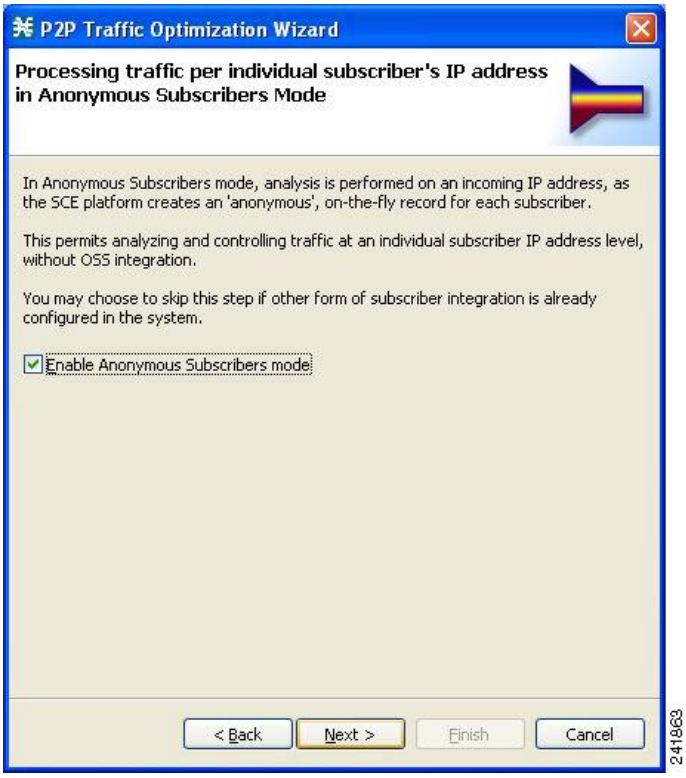


Note If a connection to one or more of the devices cannot be made or if there is some problem with the connection (such as invalid version of the device), an error is displayed next to the device. You can skip these tests by clicking Skip connectivity test. The connections are validated when you click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

Step 10 Click Next .

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

Figure 49: Anonymous Subscribers

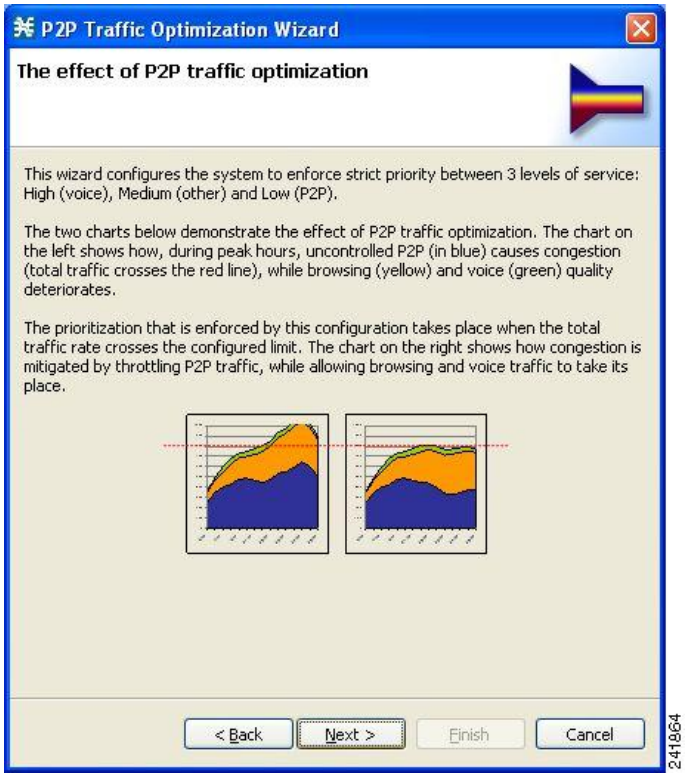


Step 11 To disable anonymous subscriber mode, uncheck the Enable Anonymous Subscribers mode check box.

Step 12 Click Next .

The effect of P2P traffic optimization page of the P2P Traffic Optimization wizard opens. This page explains why you should optimize (limit) P2P traffic.

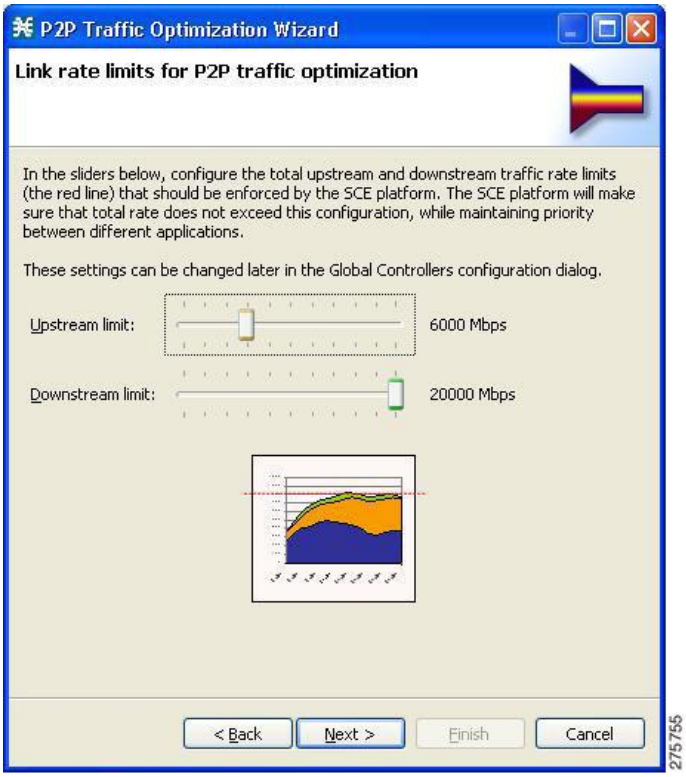
Figure 50: Effect of P2P Traffic Optimization



Step 13 Click Next .

The Link Rate Limits for P2P Traffic Optimization page of the P2P Traffic Optimization wizard opens.

Figure 51: Link Rate Limits



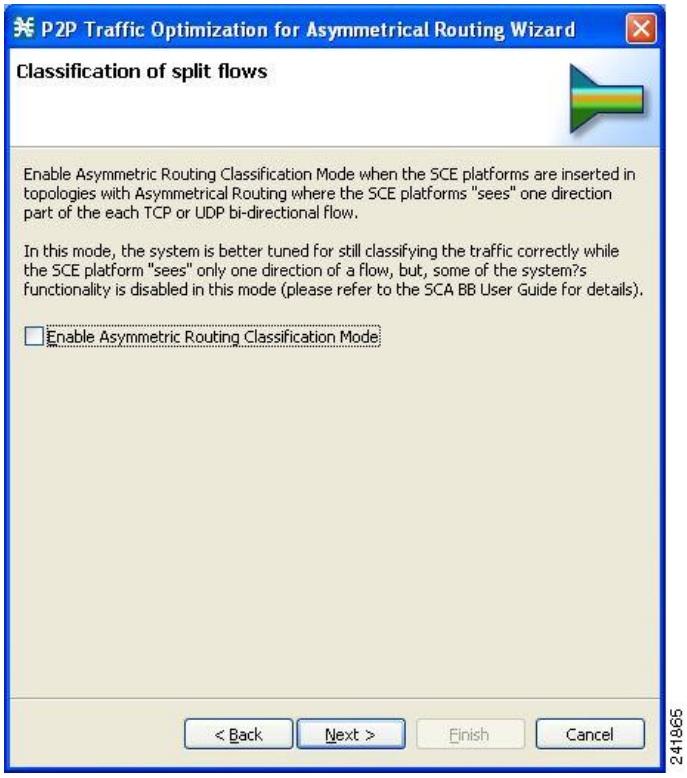
Step 14 Use the sliders to configure the upstream and downstream link rate limits.
The scale of each slider is the percentage of the aggregated bandwidth of both links.

Step 15 If you are running the P2P Traffic Optimization wizard, go to Step 20.
If you are running the P2P Traffic Optimization for Asymmetrical Routing wizard, continue at the next step.

Step 16 Click Next .

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

Figure 52: Classification of Split Flows

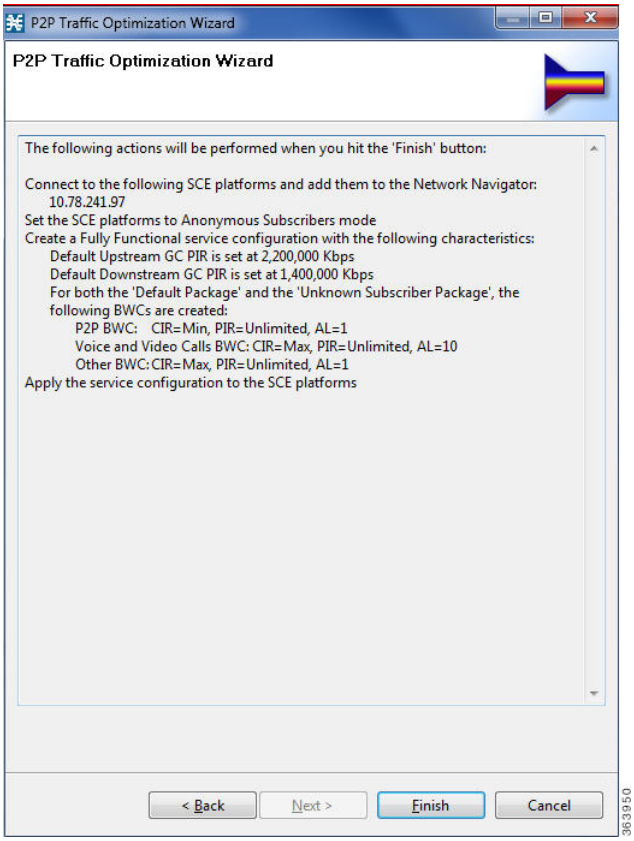


Step 17 To enable asymmetric routing classification mode, check the Enable Asymmetric Routing Classification Mode check box.

Step 18 Click Next .

The Confirmation page of the P2P Traffic Optimization wizard opens. The actions that the wizard is about to take are listed on the page.

Figure 53: Confirmation



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

For an explanation of the bandwidth controller parameters, see Subscriber BWC Parameters section .

Step 19 Click Finish .

The Configuration Output page of the P2P Traffic Optimization wizard opens. New devices are added to the default site of the Site Manager tree in the Network Navigator.

Figure 54: Configuration Output

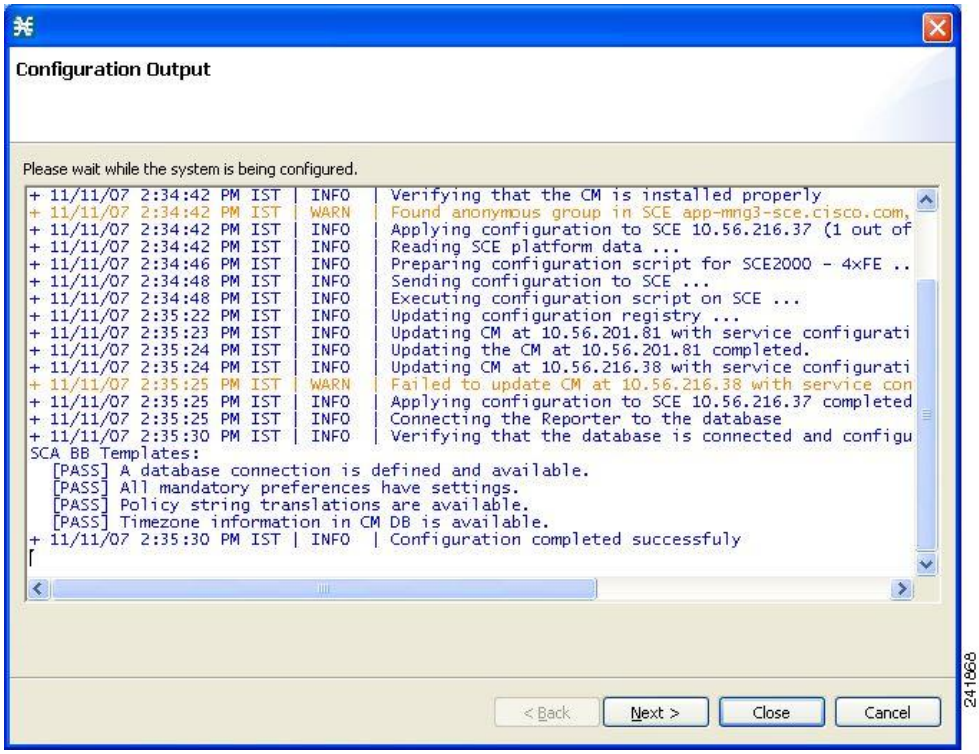
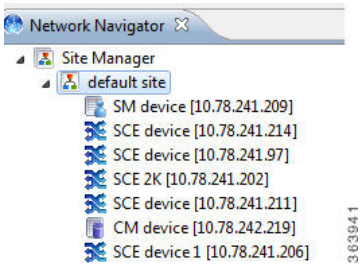


Figure 55: Network Navigator



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

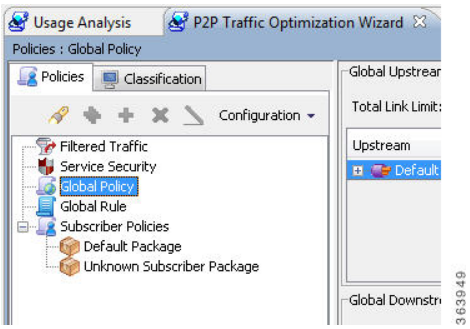
- The wizard cannot connect to any of the SCE devices that you listed in Step 4.
- You defined a CM in Step 8, but the wizard cannot connect to it.
- You defined a database in Step 10, but the wizard cannot connect to it.

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

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

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

Figure 56: Service Configuration Editor



The service configuration has the following characteristics:

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

The service configuration is applied to the SCE devices.

If you defined a database in Step 10:

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

Step 20 If you did not define a database in Step 10, click **Finish**.
The P2P Traffic Optimization wizard closes.

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

The Network Navigator Tool

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

For more information about the Network Navigator, see The Network Navigator Tool section.

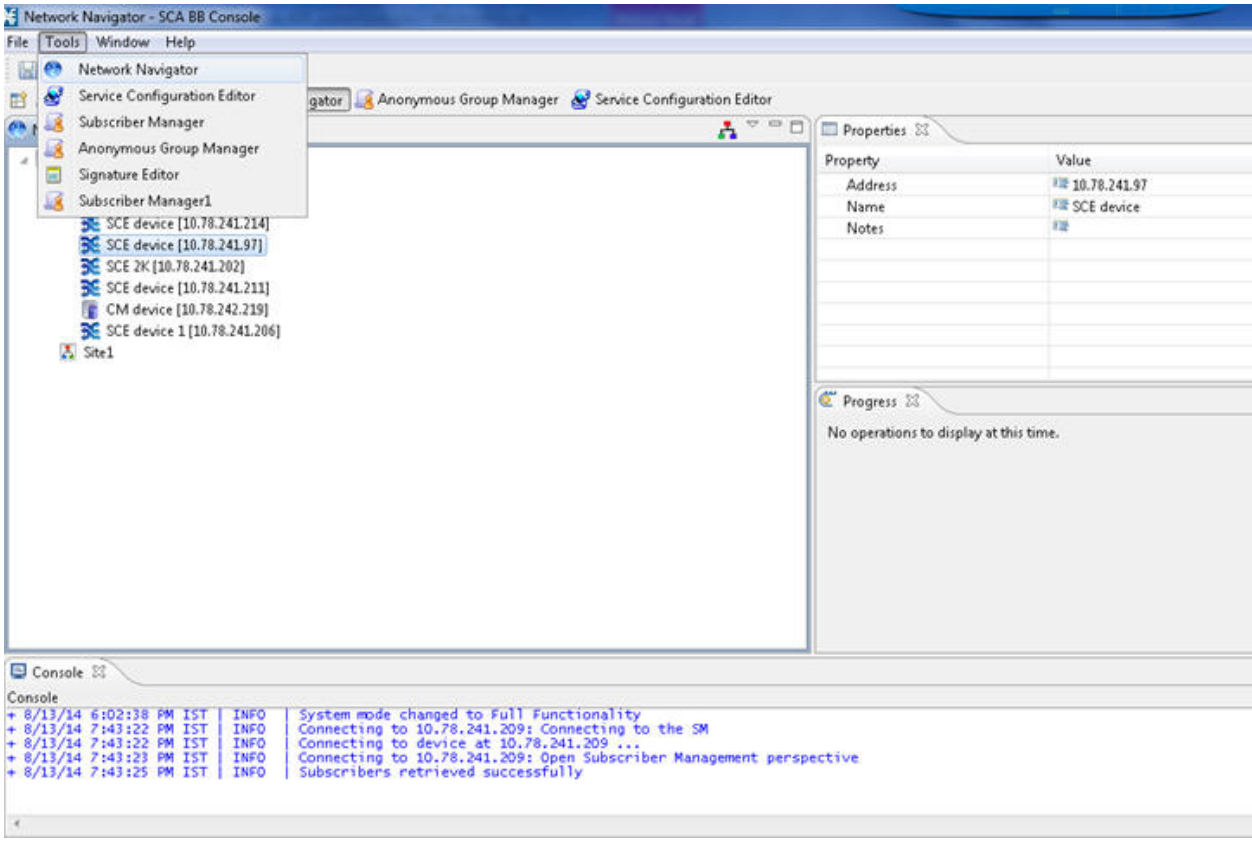
This section contains information about the following procedures:

Opening the Network Navigator Tool

Procedure

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

Figure 57: Network Navigator



Closing the Network Navigator Tool

Procedure

Step 1 Right-click the Network Navigator button.

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

The Service Configuration Editor Tool

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

Most of this document discusses using the Service Configuration Editor. See Using the Service Configuration Editor section .

Opening the Service Configuration Editor Tool

Procedure

Step 1 From the Console main menu, choose **Tools > Service Configuration Editor**.
A No Service Configuration Is Open dialog box appears.

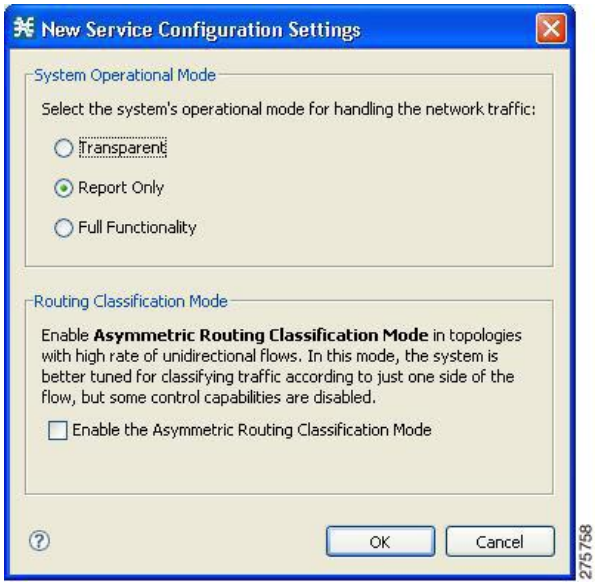
Figure 58: No Service Configuration Is Open



Step 2 Click **Yes**.

A New Service Configuration Settings dialog box appears

Figure 59: New Service Configuration Settings



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

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

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

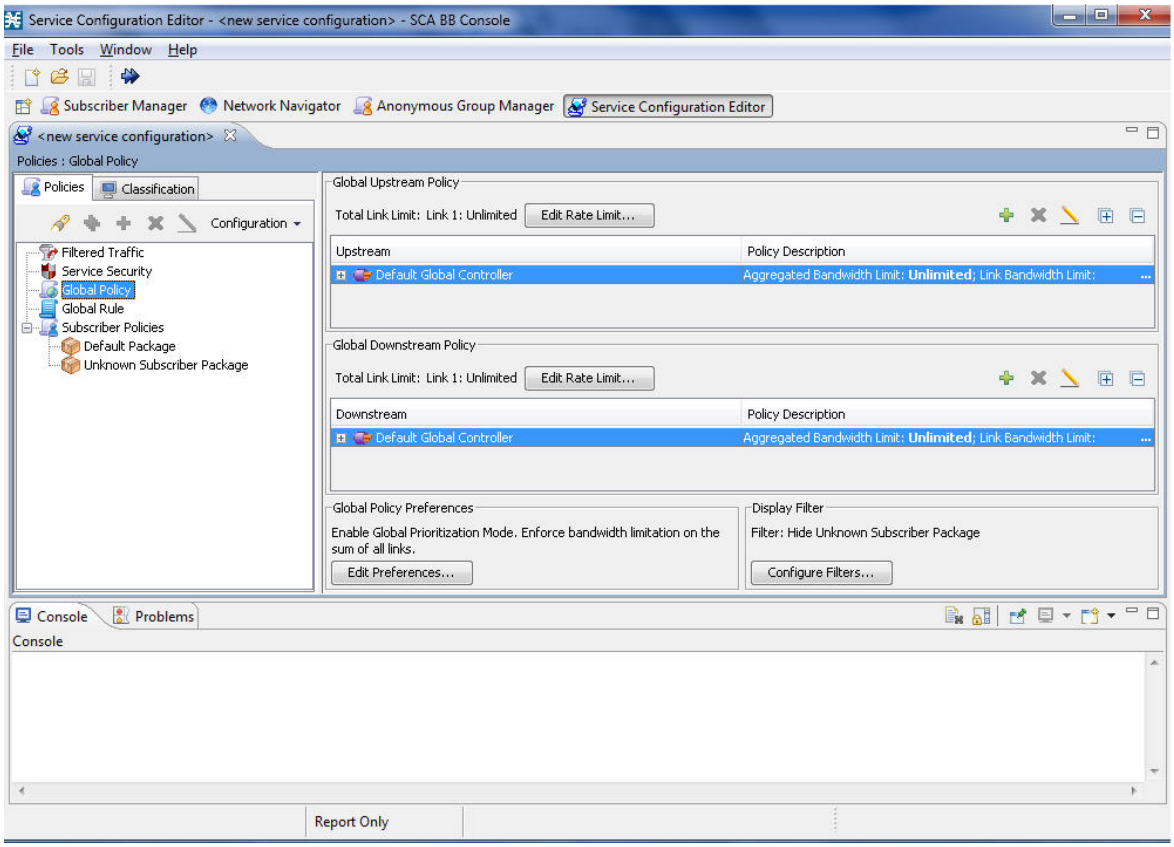
Step 4 (Optional, but highly recommended if your system has a high proportion of unidirectional flows) To switch to asymmetric routing classification mode, check the Enable the Asymmetric Routing Classification Mode check box.

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

Step 5 Click **OK**.

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

Figure 60: Service Configuration Editor



Closing the Service Configuration Editor Tool

Procedure

Step 1 Right-click the Service Configuration Editor button.

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

The Signature Editor Tool

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

For more information about the Signature Editor, see The Signature Editor Overview section.

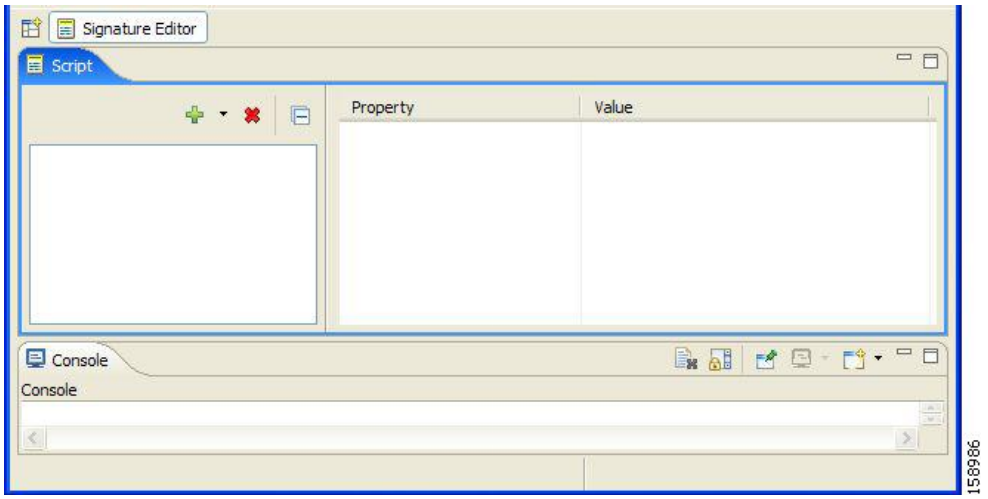
This section contains information about the following procedures:

Opening the Signature Editor Tool

Procedure

From the Console main menu, choose **Tools > Signature Editor**.
The Signature Editor tool opens.

Figure 61: Signature Editor Tool



Closing the Signature Editor Tool

Procedure

Step 1 Right-click the Signature Editor button.

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

The Subscriber Manager GUI Tool

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

For more information about connecting to a Cisco Service Control Subscriber Manager and using the Subscriber Manager GUI, see Subscriber Manager GUI Tool section .

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

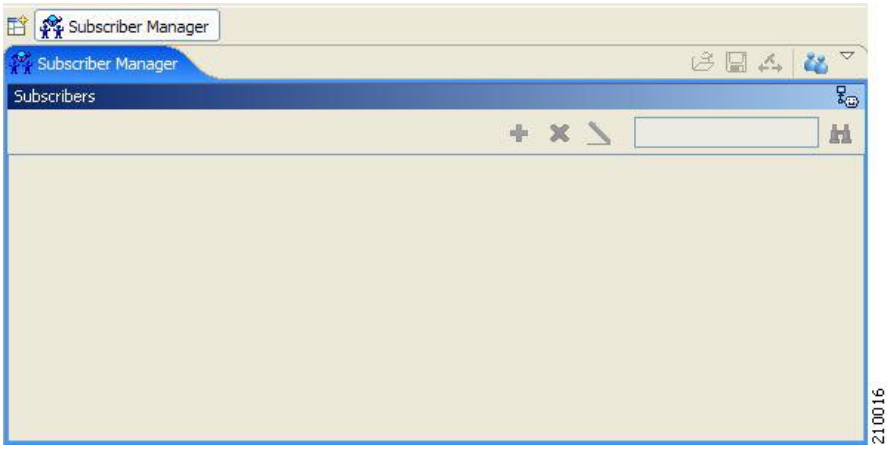
This section contains information about the following procedures:

Opening the Subscriber Manager GUI Tool

Procedure

From the Console main menu, choose Tools > Subscriber Manager .
The Subscriber Manager GUI tool opens.

Figure 62: Subscriber Manager



Closing the Subscriber Manager GUI Tool

Procedure

Step 1 Right-click the Subscriber Manager button.

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

The Anonymous Group Manager Tool

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

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

Opening the Anonymous Group Manager Tool

Procedure

From the Console main menu, choose Tools > Anonymous Group Manager .
The Anonymous Group Manager tool opens.

Closing the Anonymous Group Manager Tool

Procedure

Step 1 Right-click the Anonymous Group Manager button.
Step 2 From the popup menu that appears, select Close.

Online Help

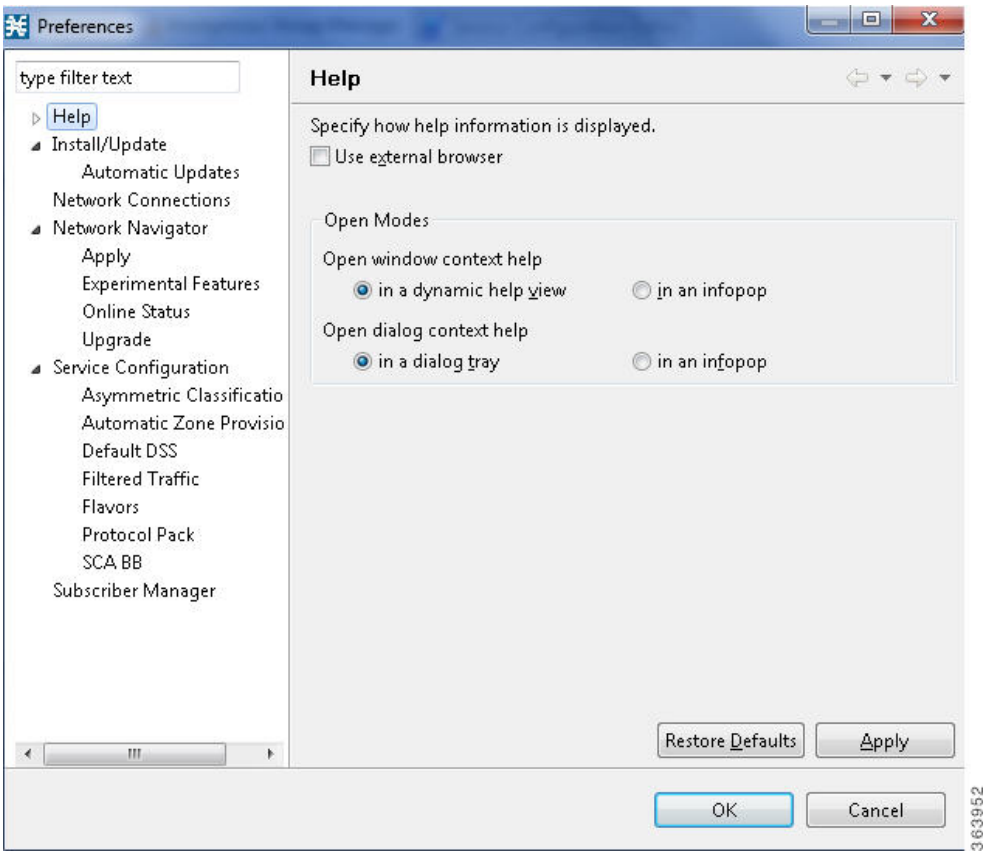
You can access relevant parts of this user guide from the Console. The following sections provide you with the necessary details:

Accessing the Online Help

Procedure

From the Console main menu, choose Help > Help Contents .

Figure 63: Preferences - Help



Online help opens in a separate window.

Searching Online Help

Procedure

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

The Help view opens next to the current tool.

Figure 64: Help



Step 2 Enter a word, phrase, or more complex search expression in the Search expression field.
The Go button is enabled.
Note Click >> (Expand) for an explanation of how to construct search expressions.

Step 3 Click Go .
Help topics containing your search expression are listed under Local Help.

Step 4 Click a help topic to view its contents.
Note You can bookmark topics for later reference.

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

- All topics
- Related topics
- Bookmarks

QuickStart with the Cisco SCA BB Console

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

Configuring the Console and Applying the Default Service Configuration

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

Procedure

Step 1 Launch the Console.
Choose **Start > All Programs > Cisco SCA > SCA BB Console 5.2.x > SCA BB Console 5.2.x**. Here x stands for the version within 5. For example, 5.2.0

Step 2 If necessary, close the Welcome view.

Step 3 Open the Network Navigator.

Step 4 From the Console main menu, choose **Tools > Network Navigator**.
This step sets up the Console for network device operations. You should now be able to see the default site displayed in the Network Navigator view.
Note The Network Navigator tool is open the first time you launch the Console.

Step 5 Add a Cisco SCE device to the default site.

a) Right-click the default site, and, from the popup menu that appears, select **New > SCE**.
The Create new SCE wizard appears.
b) In the Address field, enter the actual IP address of an SCE platform.
c) Click **Finish**.
The Create new SCE wizard closes. The new device is added to the site.

Step 6 Check the SCE platform version and operational state.

a) Right-click the SCE device and, from the popup menu that appears, select **Online Status**.
A Password Management dialog box appears.
b) Enter the username and password for managing the SCE.
c) Enter the SNMP RO Community String.
d) Click **Extract**.
The SCE online status is retrieved.
e) Check that the system and application versions are correct, and that the operational state is Active.

Step 7 Open the Service Configuration Editor.

a) From the Console main menu, choose **Tools > Service Configuration Editor**.
The Service Configuration Editor opens. A No Service Configuration Is Open dialog box appears.

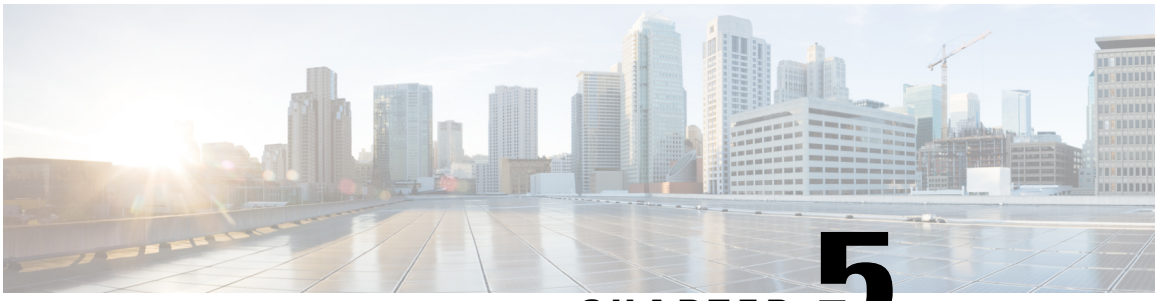
Step 8 Create a new service configuration.

a) From the Console main menu, choose **Tools > Service Configuration Editor**.
The Service Configuration Editor opens. A No Service Configuration Is Open dialog box appears.
b) Click **Yes** in the No Editor Is Open dialog box.
A New Service Configuration Settings dialog box appears.
c) Click **OK**.
A default service configuration opens in the Service Configuration Editor tool.

Step 9 Apply the service configuration to the SCE platform.

a) From the toolbar, select the Apply Service Configuration to SCE Devices ( ) icon.
A Password Management dialog box appears.
b) Enter the username and password for managing the SCE and click **Apply**.

The service configuration is applied to the SCE platform.



CHAPTER 5

The Network Navigator

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

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

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

This chapter consists of these sections:

- The Network Navigator Tool , page 107
- Introduction to Managing Sites, page 108
- Introduction to Managing Devices , page 112
- Working with Network Navigator Configuration Files , page 132
- Network Settings Requirements , page 137

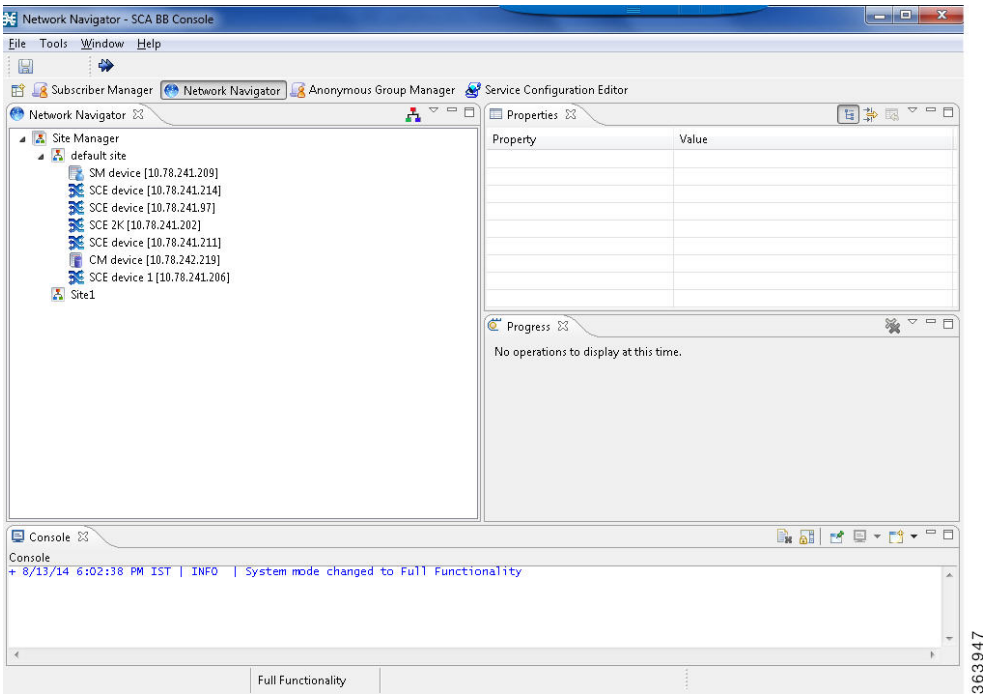
The Network Navigator Tool

The Network Navigator tool contains four views:

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

• Console view—Displays log messages concerning actions performed in the Network Navigator tool.

Figure 65: The Network Navigator Tool



Introduction to Managing Sites

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

You can also perform operations on a group of devices. For example, you can apply the same service configuration to a group of Cisco SCE platforms. The Network Navigator enables 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 112section).

This section explains these procedures:

Adding a Site to the Site Manager

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

Procedure

Step 1 In the Network Navigator view, right-click the Site Manager node.
A popup menu appears.

Figure 66: Site Manager Menu



Step 2 From the menu, select New > Site .
A new Site node is added to the Site Manager.

Step 3 In the Properties view, enter a name for the site in the Name cell.

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

Introduction to Adding Devices to a Site

You can add Cisco SCE, Subscriber Manager, CM, or database devices to a site.

Adding Cisco SCE Devices to a Site

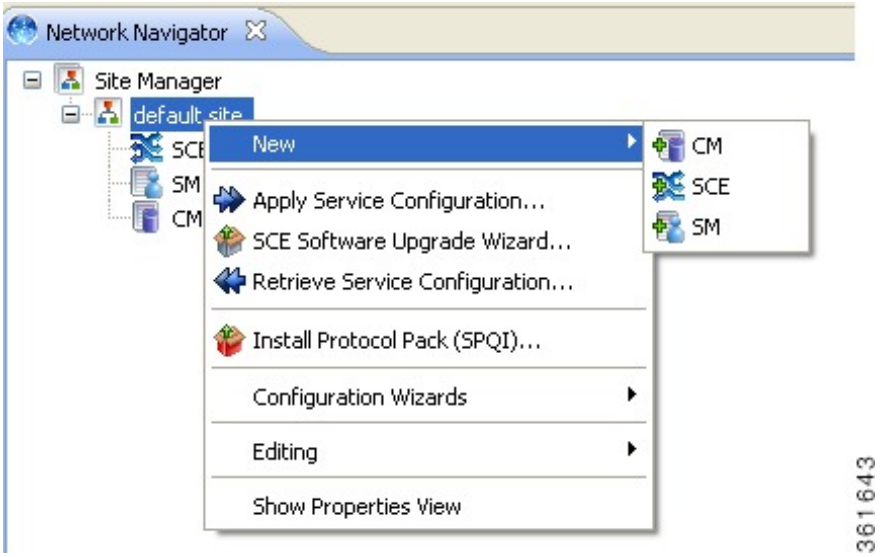
To use the Network Navigator to configure, monitor, and update the software of a Cisco SCE platform, you must first add the Cisco SCE platform to a site.

Procedure

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

A popup menu appears.

Figure 67: Site Manager Tree Menu



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 Cisco SCE.

Step 4 (Optional) In the Name field, enter a meaningful name for the Cisco SCE.

Step 5 Click Finish.
The Create New SCE wizard closes.

The new device is added to the site.

Adding Subscriber Manager Devices to a Site

To use the Network Navigator to configure, monitor, and update the software of an Subscriber Manager, you must first add the Subscriber Manager to a site.

Procedure

Step 1 In the Site Manager tree, right-click a site.
A popup menu appears.

Step 2 From the menu, select New > SM .
The Create New SM wizard appears.

Step 3 In the Address field, enter the IP address of the Cisco Service Control Subscriber Manager.

Step 4 (Optional) In the Name field, enter a meaningful name for the Subscriber Manager.

Step 5 Click Finish.

The Create New SM wizard closes.

The new device is added to the site.

Adding Collection Manager Devices to a Site

To use the Network Navigator to monitor a Collection Manager, you must first add the Collection Manager to a site.

Procedure

Step 1 In the Site Manager tree, right-click a site.
A popup menu appears.

Step 2 From the menu, select **New > CM**.
The Create New CM wizard appears.

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

Step 4 (Optional) In the Name field, enter a meaningful name for the Collection Manager.

Step 5 Click **Finish**.
The Create New CM wizard closes.

The new device is added to the site.

Deleting Devices

Procedure

Step 1 In the Site Manager tree, right-click a device.
A popup menu appears.

Step 2 From the menu, select Delete .
The device is deleted and removed from the Site Manager tree.

Deleting Sites

Procedure

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

A popup menu appears.

Step 2 If prompted, enter your password.

Step 3 From the menu, select Delete .
The site and all its devices are deleted and the site is removed from the Site Manager tree.

Introduction to Managing Devices

The Network Navigator enables you to manage Cisco SCE, Cisco Service Control Subscriber Manager, Cisco Service Control Collection Manager, and database devices.

Note The Usage Analysis wizard enables you to create a simple model of devices and connect to those devices to perform various tasks. (See Using the Usage Analysis Wizard , on page 70 section.)

This section contains these topics:

Password Management

Normally, before you can access a device (Cisco SCE, Cisco Service Control Subscriber Manager, Cisco Service Control Collection Manager, or database), you must enter its password. When you try to perform any operation on a site device, the Network Navigator first asks for the device username and password. (Repeating the same operation on the same device does not always require a second entry of the password.)

When performing operations on multiple devices, password entry can become tedious. The Site Master Password can help you remember some or all usernames and passwords of your element by storing them as part of the site data, and entering them for you automatically when you connect to an element.

The Site Master Password protects saved usernames and passwords in the password manager. The Password Management dialog box prompts you for the master password of the site when you wish to activate the site password manager. If you have multiple sites, each site requires a separate master password.

Figure 68: The Password Management Dialog Box

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

Introduction to Managing Cisco SCE Devices

This section explains the following procedures:

Configuring Cisco SCE and Collection Manager Devices Using a Wizard

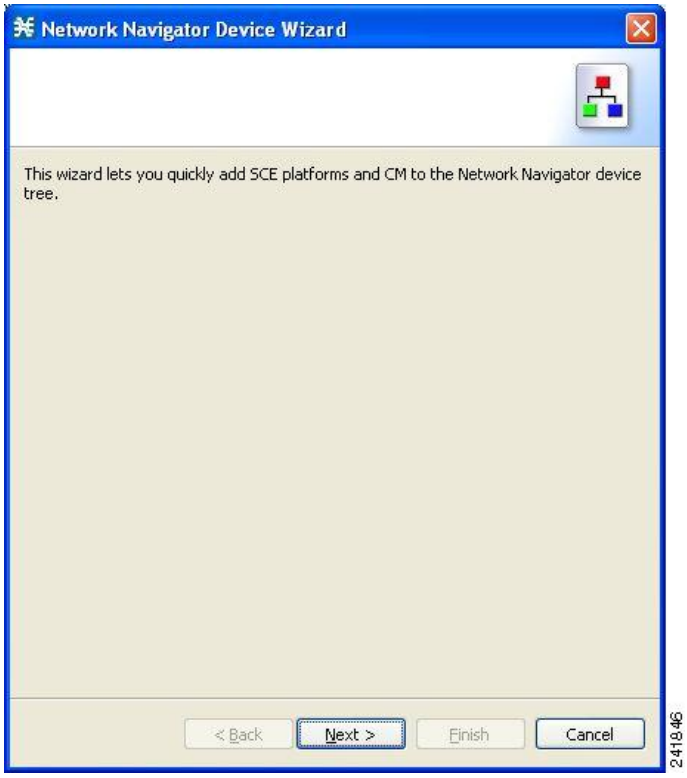
The Network Navigator Device wizard allows you to configure Cisco SCE and Cisco Service Control Collection Manager devices and connect to them.

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

Procedure

Step 1 In the Network Navigator view toolbar, click the Configure SCE and CM devices ( ) icon. The Welcome window of the Network Navigator Device wizard appears.

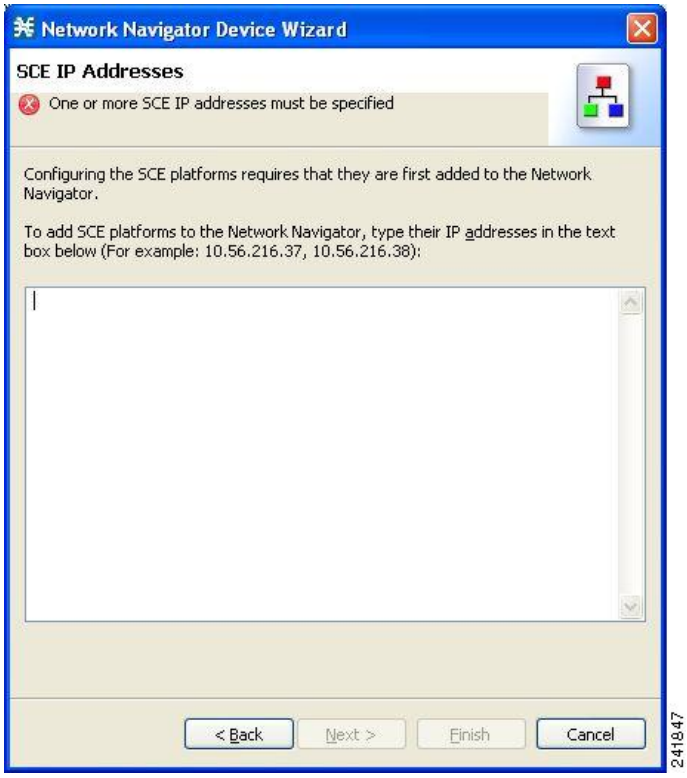
Figure 69: Welcome - Network Navigator Device



Step 2 Click **Next**.

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

Figure 70: SCE IP Addresses



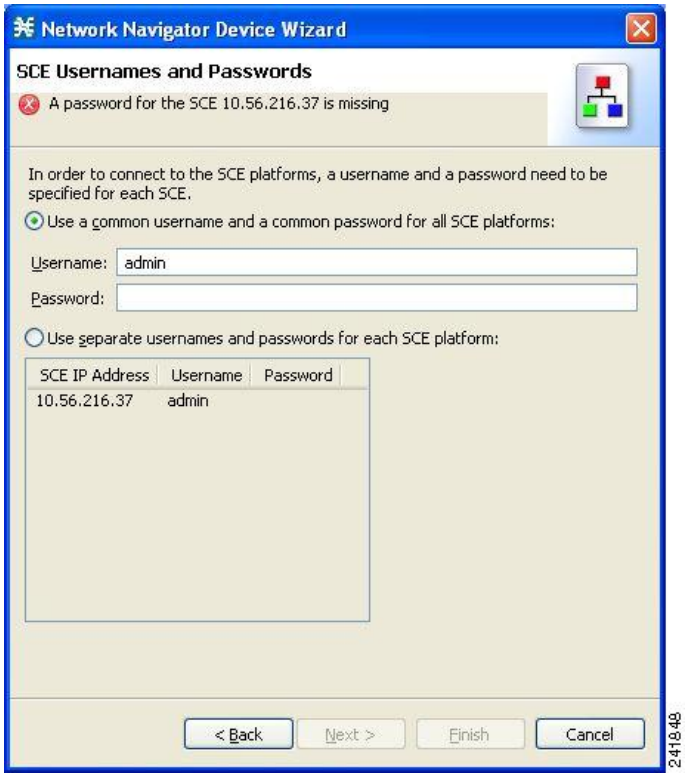
Step 3 In the edit box, enter the IP addresses of the Cisco SCE devices that should be added to the model.
If you started from the Network Navigator, the IP addresses of the Cisco SCE devices that you selected are displayed in the edit box. You can add additional addresses.

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

Step 4 Click **Next**.

The SCE Usernames and Passwords page of the Network Navigator Device wizard opens.

Figure 71: SCE Usernames and Passwords



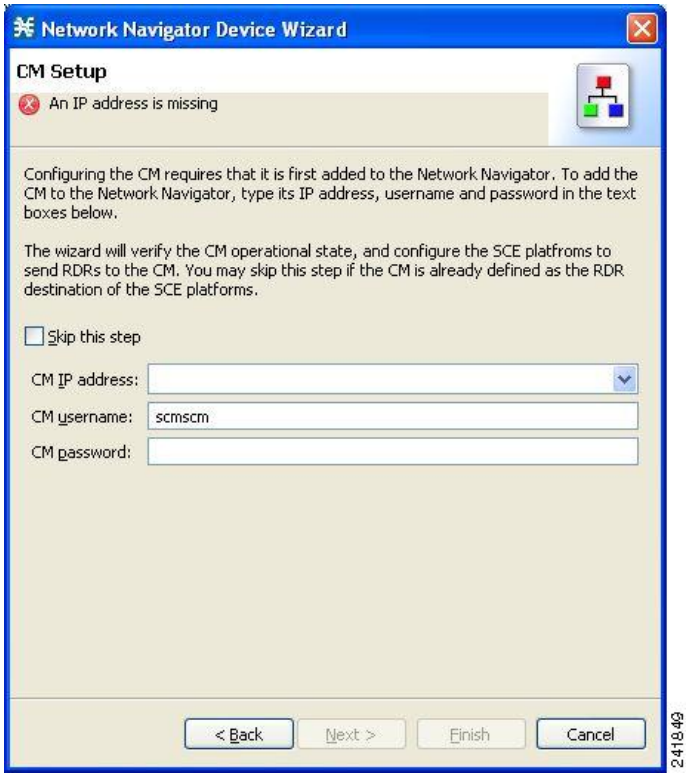
Step 5 Enter the usernames and passwords for the Cisco SCE devices.
Do one of the following:

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

Step 6 Click **Next**.

The Cisco Service Control Collection Manager Setup page of the Network Navigator Device wizard opens.

Figure 72: Cisco Service Control Collection Manager Setup



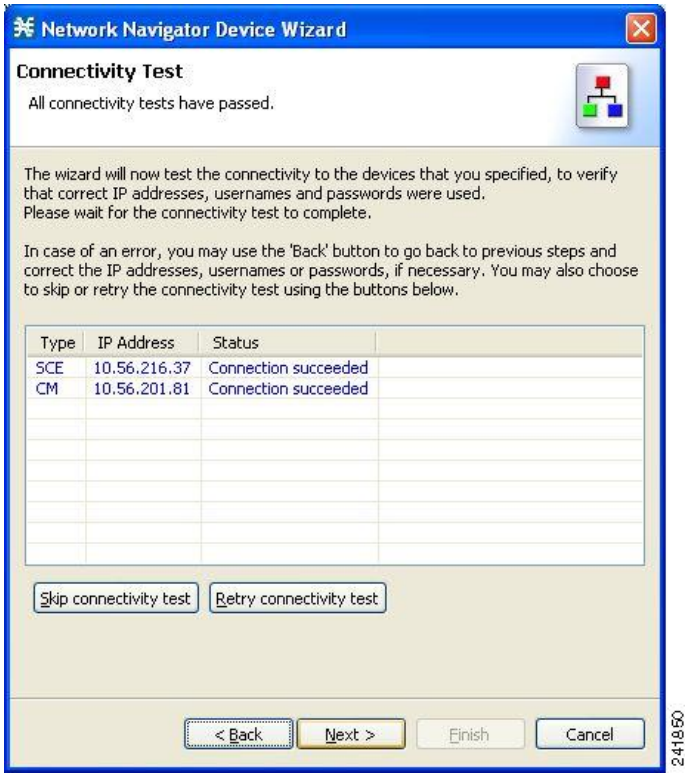
Step 7 Define the Cisco Service Control Collection Manager to use with this configuration.
Do one of the following:

- Enter the IP address, username, and password of the CM device in the appropriate fields.
  If you started from the Network Navigator, this information is retrieved and displayed. You can modify these parameters.
- Check the Skip this step check box.

Step 8 Click **Next**.

The Connectivity Test page of the Network Navigator Device wizard opens.

Figure 73: Connectivity Test



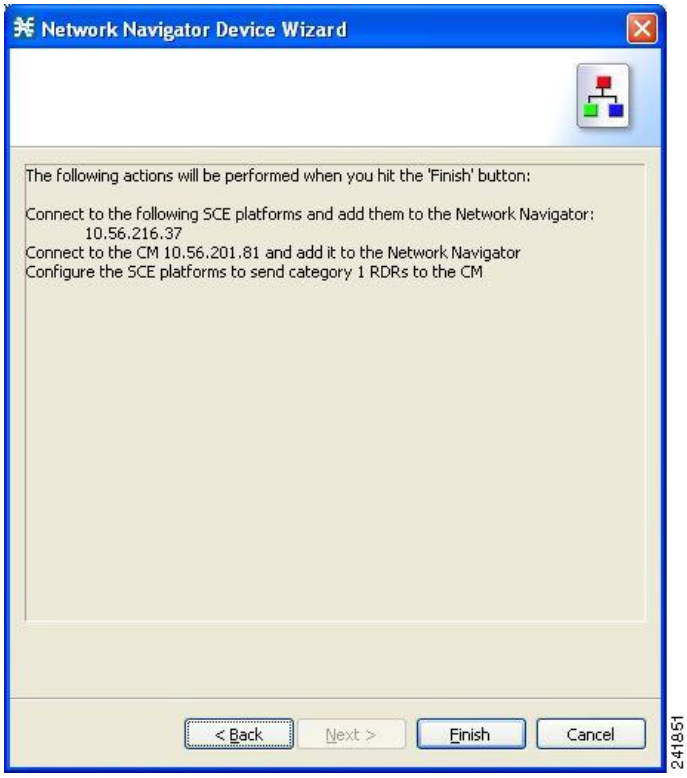
The wizard tests to see that the connections to the defined devices can be made.

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

Step 9 Click **Next**.

The Confirmation page of the Network Navigator Device wizard opens.

Figure 74: Confirmation

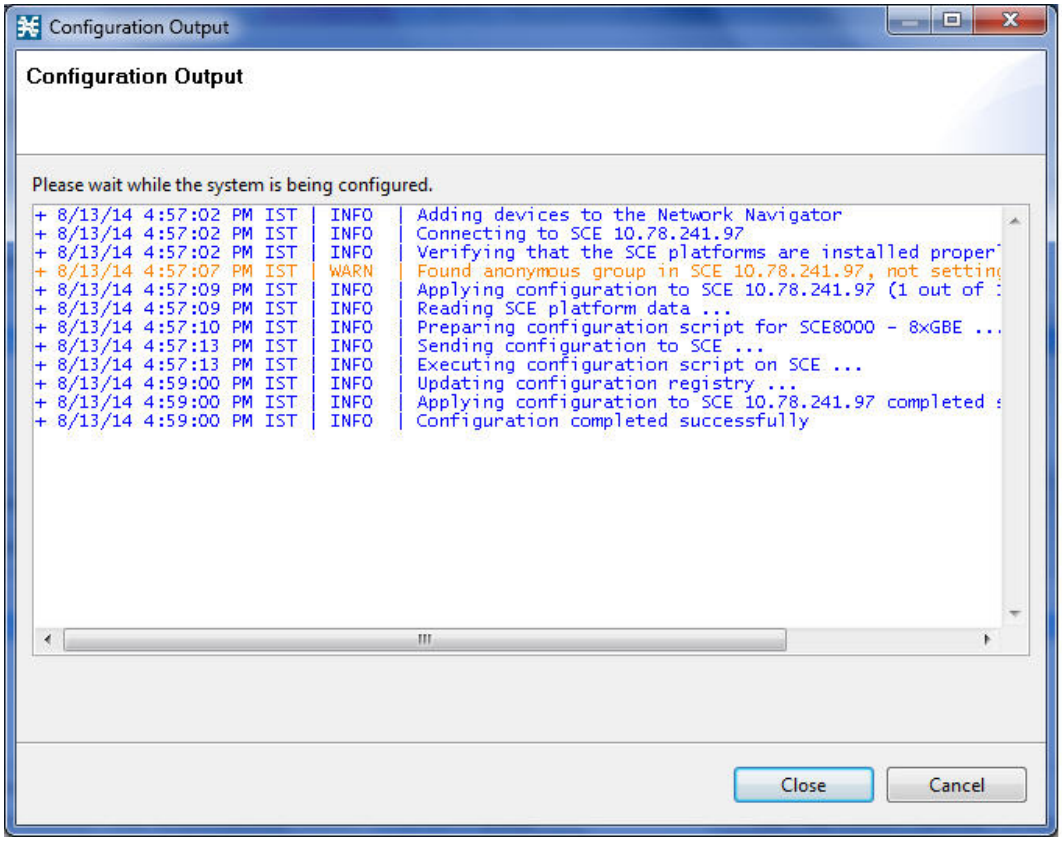


The actions that the wizard is about to take are listed on the page.

Step 10 Click **Finish**.

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

Figure 75: Configuration Output



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

Figure 76: Network Navigator



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

- The wizard cannot connect to any of the Cisco SCE devices that you listed in Step 3.
- You defined a CM in Step 7, but the wizard cannot connect to it.

If you defined a CM in Step 7, the Cisco SCE devices are configured so that the only category 1 RDR destination is the CM.

A new service configuration is created:

- Report Only mode.
- The maximum Transaction RDR rate is set as the default value (250) divided by the number of Cisco SCE devices. (To configure the Transaction RDR, see Managing Transaction RDRs, on page 256 section ; the content and structure of the Transaction RDR is listed in the "Transaction RDR" section in the "Raw Data Records: Formats and Field Contents" chapter of *Cisco Service Control Application for Broadband Reference Guide.)*

Step 11 Click **Finish**.
The Network Navigator Device wizard closes.

Generating Tech Support Info Files for Cisco SCE Devices

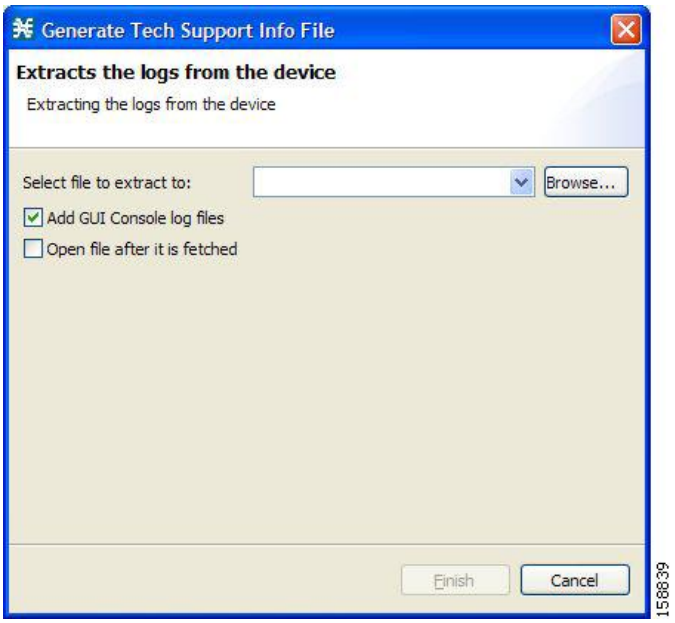
This operation generates the support file, for the Cisco SCE platform, for the use of Cisco technical support staff.

Procedure

Step 1 In the Site Manager tree, right-click an SCE device.
A popup menu appears.

Step 2 From the Site Manager Tree menu, select Generate Tech Support Info File .
The Generate Tech Support Info File dialog box appears.

Figure 77: Generate Tech Support Info File



Step 3 Click Browse.

A Select File dialog box appears.

Step 4 Browse to the folder where you want to save the tech support info file.

Step 5 In the File name field, enter a new file name, or select an existing ZIP file.

Step 6 Click Open to select the file.
If the file exists, it is overwritten when you generate the tech support info.

The Select File dialog box closes.

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

Step 8 (Optional) Check the Open file after it is fetched check box.

Step 9 Click Finish.
The Generate Tech Support Info File dialog box closes.

A Password Management dialog box appears.

Step 10 Enter the appropriate password. (For more information, see Password Management , on page 112 section.)

Step 11 Click Generate.
The Password Management dialog box closes.

A Generate tech support info file progress bar appears.

The file is generated.

Retrieving the Online Status of Cisco SCE Devices

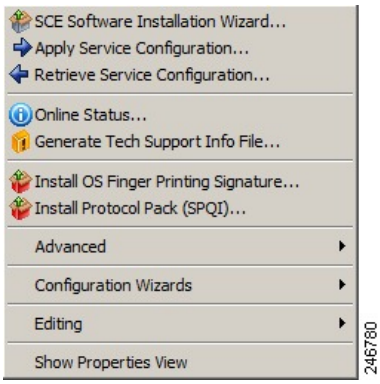
This operation provides information about the current software version and operational status of the Cisco SCE platform. The enhanced Cisco SCE online statuses are categorized as:

- System—displays the platform information
- Configuration—displays the Hostname
- Status—displays the operational mode and total traffic on the Cisco SCE

For more information on monitoring Cisco SCE online status, see the Cisco SCA BB Demo Kit Quick Start Guide.

Procedure

Step 1 In the Site Manager tree, right-click an SCE device.
A popup menu appears.



Step 2 From the menu, select **Online Status**.
A Password Management dialog box appears.

Step 3 Enter the appropriate password.
For more information, see Password Management , on page 112 section.

Step 4 Enter the SNMP RO Community String.
If SNMP is not already enabled on the Cisco SCE, it gets enabled.

If RO communities are not configured on the Cisco SCE or if only RW communities are configured on the Cisco SCE, the SNMP RO community you provide here is added to the Cisco SCE.

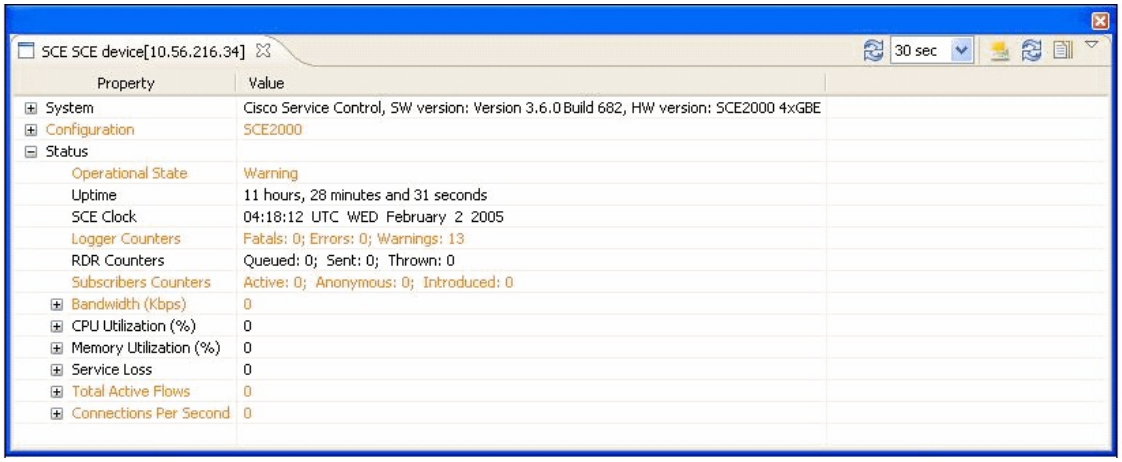
If only RO communities are configured on the Cisco SCE, the SNMP RO community you provide here is validated first against the RO communities configured on Cisco SCE. If the RO community is valid, the online status window is launched. If the RO community is not valid, a validation message appears.

Step 5 Click Extract .
The Password Management dialog box closes.

An Extracting info progress bar appears.

The Cisco SCE online status is retrieved.

Figure 78: Cisco SCE Online Status



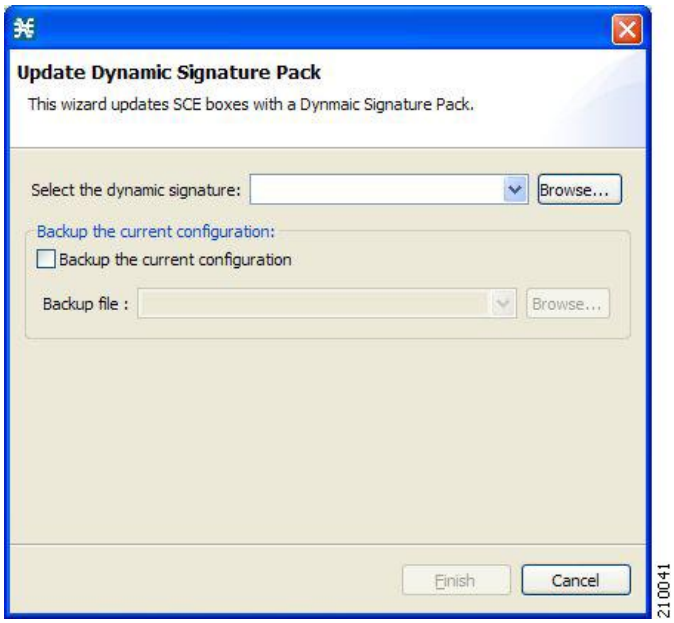
Installing a Protocol Pack on a Single Cisco SCE Platform

Procedure

Step 1 In the Site Manager tree, right-click the Cisco SCE on which you plan to install the protocol pack.

Step 2 From the popup menu that appears, select Update Dynamic Signature Pack .
The Update Dynamic Signature Pack dialog box appears.

Figure 79: Update Dynamic Signature Pack



Step 3 Click Browse.
A Select file dialog box appears.

Step 4 From the Files of type drop-down list, select *.spqi or *.dss , depending on the file to be installed.

Step 5 Browse to the file to be installed.

Step 6 Click Open.
The Select file dialog box closes.

Step 7 (Recommended) Check the Backup the current configuration check box, click Browse , and select a backup file.

Step 8 Click Finish.
A Password Management dialog box appears.

Step 9 Enter the appropriate password.
For more information, see Password Management , on page 112 section.

Step 10 Click Update.
The Password Management dialog box closes.

An Update Dynamic Signature Pack progress bar appears.

The service configuration on the Cisco SCE platform is updated.

Introduction to Applying Service Configurations to Cisco SCE Devices

You can apply a service configuration to a single Cisco SCE platform, to selected Cisco SCE platforms, or to all Cisco SCE platforms at one or more selected sites.

Note The service configuration that you are applying must be open in the Service Configuration Editor.

Caution If anomaly-based detection of malicious traffic is enabled, any access control list (ACL) that is configured on the Cisco Service Control Engine (Cisco SCE) platform but is not applied to anything (for example, an interface, an access map, or an SNMP community string) might be deleted when a service configuration is applied to the platform. To workaround this issue, disable anomaly-based detection of malicious traffic. In the Network Traffic tab, select Service Security . In the Service Security Dashboard, clear the Enable anomaly detection check box.

Applying a Service Configuration to Multiple Cisco SCE Platforms

Procedure

Step 1 In the Site Manager tree, select sites or Cisco SCE devices to which you are applying the service configuration and right-click one of them.

Step 2 From the popup menu that appears, select Apply Service Configuration.
The Choose Policy dialog box appears, listing all service configurations that are open in the Service Configuration Editor.

Note If only one service configuration is open in the Service Configuration Editor, a Password Management dialog box appears. Continue at Step 4. (If no service configurations are open in the Service Configuration Editor, an error message is displayed.)

Step 3 Select a service configuration from the list and click OK.
A separate Password Management dialog box appears for each Cisco SCE device that you have selected.

Step 4 For each Cisco SCE device, enter the password and click Apply .
The service configuration is applied to each selected Cisco SCE platform in turn.

Applying a Service Configuration to a Single Cisco SCE Platform

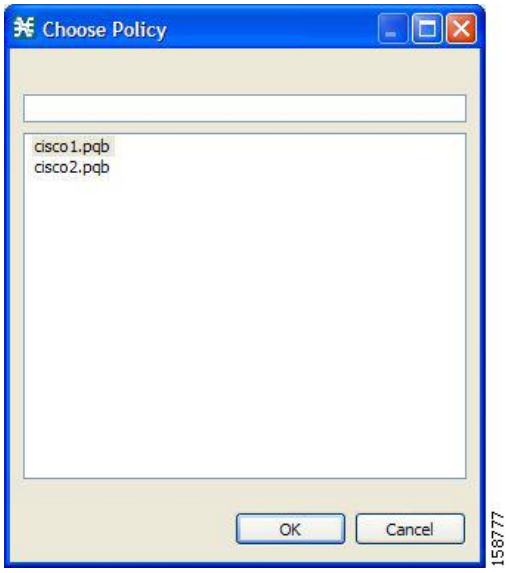
Procedure

Step 1 In the Site Manager tree, right-click a Cisco SCE device.
A popup menu appears.

Step 2 From the menu, select Apply Service Configuration .
The Choose Policy dialog box appears, listing all service configurations that are open in the Service Configuration Editor.

Note If only one service configuration is open in the Service Configuration Editor, a Password Management dialog box appears. Continue at Step 5. (If no service configurations are open in the Service Configuration Editor, an error message is displayed.)

Figure 80: Choose Policy



Step 3 Select a service configuration from the list.

Step 4 Click OK.
A Password Management dialog box appears.

Step 5 Enter the appropriate password. (For more information, see Password Management , on page 112 section)

Step 6 Click Apply.
The Password Management dialog box closes.

An Applying service configuration to Cisco SCE progress bar appears.

The service configuration is applied to the selected Cisco SCE platform.

Introduction to Retrieve Service Configurations from Cisco SCE Devices

You can retrieve service configurations from a single Cisco SCE platform, from selected Cisco SCE platforms, or from all Cisco SCE platforms at one or more selected sites.

Retrieving Service Configurations from Multiple Cisco SCE Platforms

Procedure

Step 1 In the Site Manager tree, select sites or Cisco SCE devices whose service configurations you want to retrieve, and right-click one of them.

Step 2 From the popup menu that appears, select Retrieve Service Configuration.
A separate Password Management dialog box appears for each Cisco SCE device that you have selected.

Step 3 For each Cisco SCE device, enter the password and click Retrieve .
The service configuration is retrieved from each Cisco SCE platform in turn, and is opened in the Service Configuration Editor.

Retrieving Service Configurations from a Single Cisco SCE Platform

Procedure

Step 1 In the Site Manager tree, right-click a Cisco SCE device.
A popup menu appears.

Step 2 Enter your password if prompted.

Step 3 From the menu, select Retrieve Service Configuration .
A Password Management dialog box appears.

Step 4 Enter the appropriate password.
For more information, see Password Management , on page 112 section.

Step 5 Click Retrieve .
The Password Management dialog box closes.

A Retrieving from Cisco SCE progress bar appears.

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

Installing PQI Files on Cisco SCE Devices

This operation installs the Cisco SCA BB on the Cisco SCE platform.

Note It is recommended to use the SCE Software Upgrade wizard when installing a PQI file on multiple Cisco SCE devices. See Upgrading the SCE Using the SCE Software Upgrade Wizard, on page 44 section.

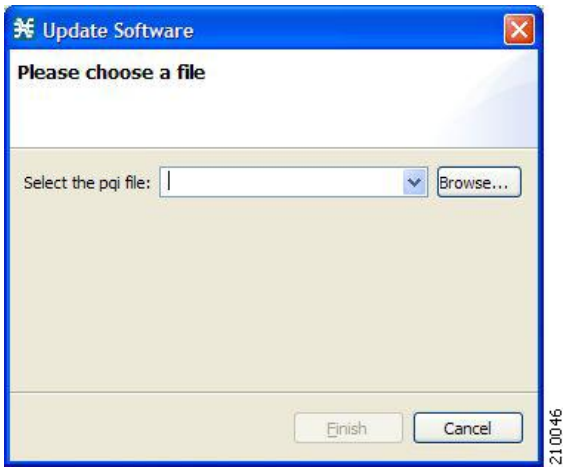
Note Installing a PQI file usually takes a few minutes.

Procedure

Step 1 In the Site Manager tree, select a Cisco SCE device.

Step 2 From the Console main menu, choose Network > Install Application Software (PQI).
The Update Software dialog box appears.

Figure 81: Update Software



Step 3 Click Browse .
A Select file dialog box appears.

Step 4 Browse to the PQI file that you are installing.

Step 5 Click Open.
The Select file dialog box closes.

Step 6 Click Finish.
A Password Management dialog box appears.

Step 7 Enter the appropriate password.
For more information, see Password Management , on page 112 section.

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 Cisco SCE.

Installing a Cisco SCE OS Software Package on Cisco SCE Devices

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

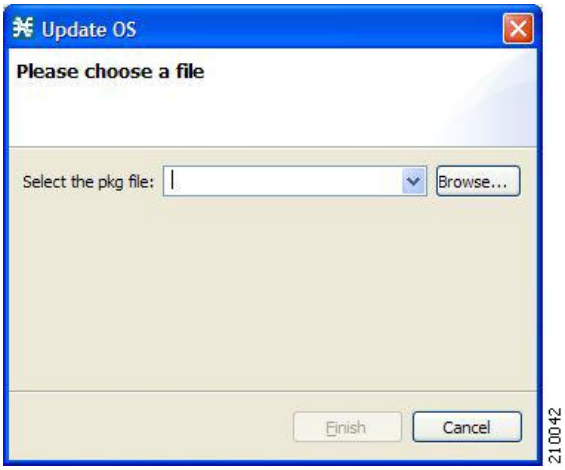
Note It is recommended to use the SCE Software Upgrade wizard when installing an SCE OS software package on multiple Cisco SCE platforms. See Upgrading the SCE Using the SCE Software Upgrade Wizard, on page 44 section.

Procedure

Step 1 In the Site Manager tree, select a Cisco SCE device.

Step 2 From the Console main menu, choose Network > Upgrade SCE Platform Firmware (PKG) .
The Update OS dialog box appears.

Figure 82: Update OS



Step 3 Click Browse .
A Select file dialog box appears.

Step 4 Browse to the PKG file containing the OS that you are installing.

Step 5 Click Open.
The Select file dialog box closes.

Step 6 Click Finish.
A Password Management dialog box appears.

Step 7 Enter the appropriate password.
For more information, see Password Management , on page 112 section.

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 Cisco SCE.

Introduction to Managing Subscriber Manager Devices

Generating Tech Support Info Files for Subscriber Manager Devices

This operation generates the support file, for the Subscriber Manager, for the use of Cisco technical support staff.

Procedure

Step 1 In the Site Manager tree, right-click an Subscriber Manager device.
A popup menu appears.

Figure 83: Site Manager Tree Menu



Step 2 From the menu, select Generate Tech Support Info File .
The Generate Tech Support Info File dialog box appears.

Step 3 Click Browse.
A Select File dialog box appears.

Step 4 Browse to the folder where you want to save the tech support info file.

Step 5 In the File name field, enter a new file name, or select an existing ZIP file.

Step 6 Click Open to select the file.
If the file exists, it is overwritten.

The Select File dialog box closes.

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

Step 8 Check the Open file after it is fetched check box.

Step 9 Click Finish.
The Generate Tech Support Info File dialog box closes.

A Password Management dialog box appears.

Step 10 Enter the appropriate password. (For more information, see Password Management , on page 112 section.)

Step 11 Click Generate.
The Password Management dialog box closes.

A Generate tech support info file progress bar appears.

The file is generated.

Retrieving the Online Status of Subscriber Manager Devices

This operation provides information about the current software version and operational status of the Subscriber Manager Device.

Procedure

Step 1 In the Site Manager tree, right-click an Subscriber Manager device.
A popup menu appears.

Step 2 From the menu, select Online Status.
A Password Management dialog box appears.

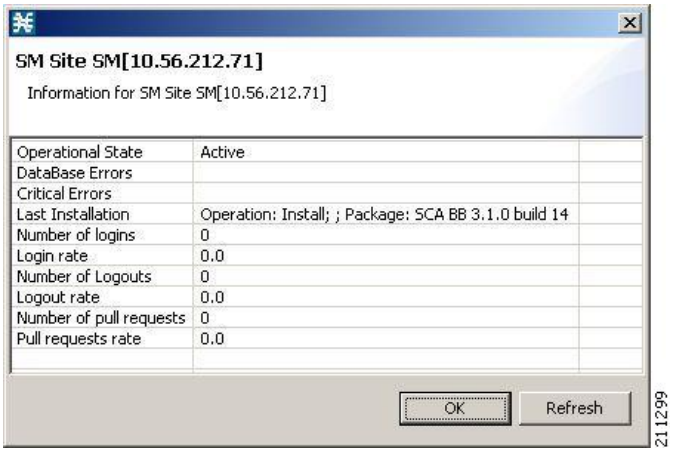
Step 3 Enter the appropriate password.
For more information, see Password Management , on page 112 section

Step 4 Click Extract.
The Password Management dialog box closes.

An Extracting info progress bar appears.

The Cisco Service Control Subscriber Manager online status is retrieved.

Figure 84: Cisco Service Control Subscriber Manager Online Status



Connecting to Subscriber Manager Devices

To manage subscribers using the Subscriber Manager GUI tool, you must connect to an Subscriber Manager device.

Note The Subscriber Manager GUI tool performs authentication on the Cisco Service Control Subscriber Manager by opening a PRPC connection to port 14374 and attempting to log in using the username and password that you entered in the Password Management dialog box. If a PRPC server with this user is not running on the Cisco Service Control Subscriber Manager, authentication fails. If you have changed the PRPC port on the Cisco Service Control Subscriber Manager, see User Authentication , on page 137 section.

Procedure

Step 1 In the Site Manager tree, right-click an Subscriber Manager device.
A popup menu appears.

Step 2 From the menu, select Manage Subscribers .
A Password Management dialog box appears.

Step 3 Enter the appropriate password. (For more information, see Password Management , on page 112 section.)

Step 4 Click Connecting.
The Password Management dialog box closes.

A Connecting to progress bar appears.

You connect to the Subscriber Manager, and the Console switches to the Subscriber Manager GUI tool.

What to Do Next

For an explanation of how to proceed, see Subscriber Manager GUI Tool, on page 457 section.

Introduction to Managing Collection Manager Devices

You can configure Collection Manager devices using a wizard. See Configuring Cisco SCE and Collection Manager Devices Using a Wizard , on page 112 section.

Retrieving the Online Status of CM Devices

This operation provides information about the current software version and operational status of the Collection Manager.

Procedure

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

A popup menu appears.

Figure 85: Site Manager Tree Menu



Step 2 From the menu, select Online Status .
A Password Management dialog box appears.

Step 3 Enter the appropriate password.
For more information, see Password Management , on page 112 section.

Step 4 Click Extract.
The Password Management dialog box closes.

An Extracting info progress bar appears.

The Cisco Service Control Collection Manager online status is retrieved.

For an example of a retrieved online status window (for a Cisco SCE platform), see Retrieving the Online Status of Cisco SCE Devices , on page 121 section .

Working with Network Navigator Configuration Files

After you add sites and devices to the Network Navigator, you can export this data to a file to back up your settings and to share them with other users, who can import your Network Navigator settings into their Console.

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

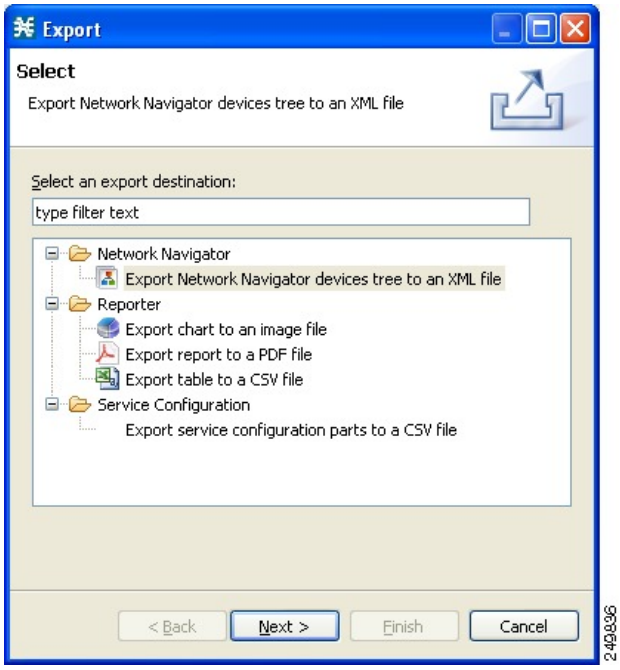
Exporting a Network Navigator Configuration

Procedure

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

The Export dialog box appears.

Figure 86: Export

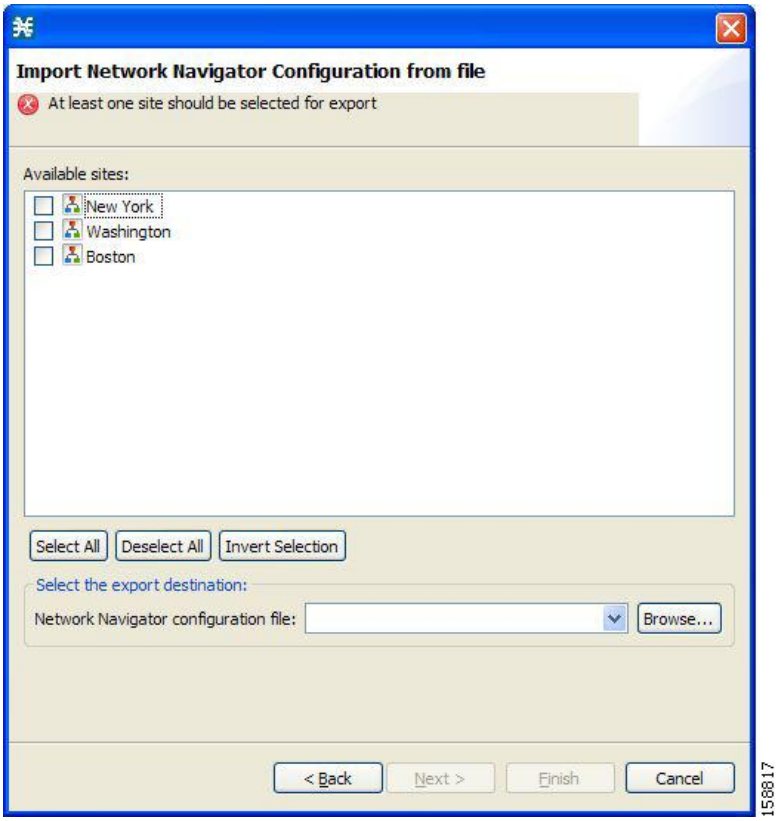


Step 2 From the export destination list, select Network Navigator Configuration to a file.

Step 3 Click Next .

The Export Network Navigator Configuration to a file dialog box appears.

Figure 87: Import Network Navigator Configuration from File



The Available sites pane lists all of the sites in the configuration.

Step 4 Select the sites to export, using the check boxes and the select buttons.

Step 5 In the Select the export destination area, click Browse.
An Open dialog box appears.

Step 6 Browse to the folder where you want to save the configuration file.

Step 7 In the File name field, enter a new file name, or select an existing site_xml file.

Step 8 Click Open to select the file.

Note If the file exists, it is overwritten.

The Open dialog box closes.

Step 9 Click Finish.
The Export Network Navigator Configuration dialog box closes.

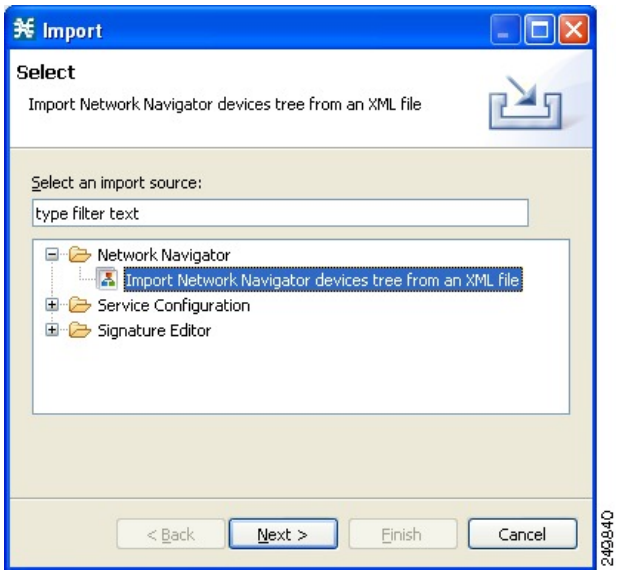
The configuration is saved to the file.

Importing a Network Navigator Configuration

Procedure

Step 1 From the Console main menu, choose File > Import .
The Import dialog box appears.

Figure 88: Import

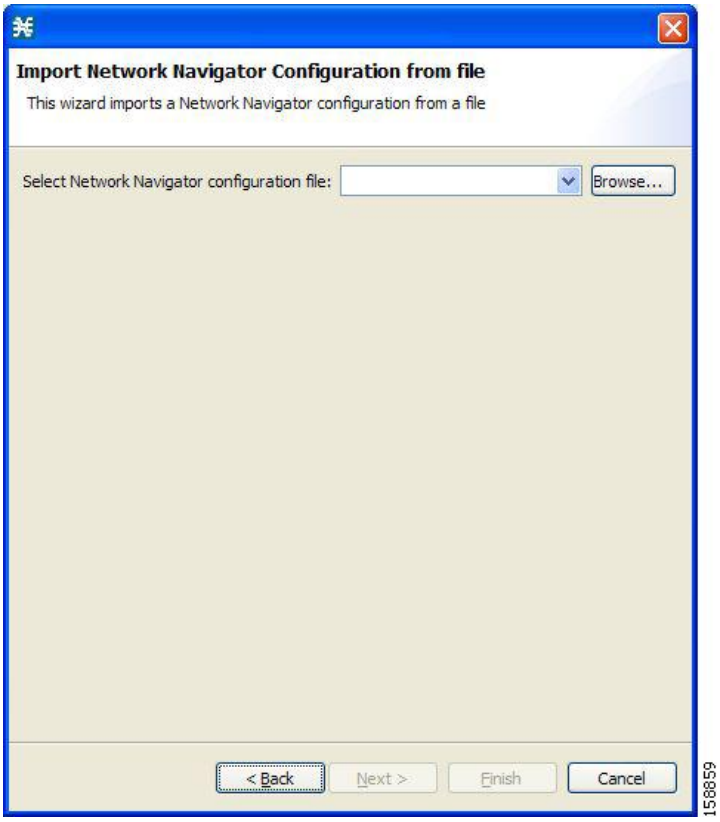


Step 2 From the import source list, select Network Navigator Configuration from file.

Step 3 Click Next.

The Import Network Navigator Configuration from file dialog box appears.

Figure 89: Import Network Navigator Configuration from File



Step 4 Click Browse.
An Open dialog box appears.

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

Step 6 Click Open to select the file.
The Open dialog box closes.

Step 7 Click Finish .
The Import Network Navigator Configuration dialog box closes.

The configuration is imported from the file.

Network Settings Requirements

Firewall and NAT Requirements

The ports listed in the table are the default values. If you change a port in a device, you must modify the firewall/NAT settings accordingly. (Modifying the Console settings to connect to a different PRPC port is described in the following section.)

Table 5: Required Firewall NAT Settings Required for Network Navigator to Operate Properly

Source	Destination	Comments
Workstation	Cisco SCE port 14374/TCP	PRPC—Required for all Cisco SCE operations
Cisco SCE	Workstation port 21/TCP	FTP—Required for the following Cisco SCE operations: • Install OS • Generate Tech Support Info File
Cisco SCE	Workstation ports 21000/TCP to 21010/TCP	FTP—Alternative to port 21/TCP, required if another application on the workstation is using port21/TCP.
Workstation	Subscriber Manager port 14374/TCP	PRPC—Required for all Subscriber Manager operations
Workstation	CM port 14375/TCP	PRPC—Required for the CM Online Status operation and for CM authentication

The SCA Reporter may have additional requirements for connecting to the database. For more information, see the Cisco Service Control Application Reporter User Guide.

User Authentication

User authentication is performed when a Proprietary Remote Procedure Call (PRPC) connection is made to a Cisco SCE platform, a CM, or an Subscriber Manager. For authentication to succeed, a PRPC server must be running at the destination, and you must know the username and password of a user of the server.

Note If you change a PRPC server port in a device (SM/CM/Cisco SCE), you must add a line to the configuration file engage.ini : <IP address of device>.rpc.port=<port number> For example: 10.56.216.37.rpc.port=222 Add one line for each (non-default) port that you use. The file engage.ini is located in the folder Program files\Cisco SCA\SCA BB Console 5.2.x\plugins\policy.contribution_5.2.x\config\ .

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

For more information about defining users, see the following:

- Collection Manager—"Managing Users" section in the "Managing the Collection Manager" chapter of Cisco Service Control Management Suite Collection Manager User Guide.
- Subscriber Manager—"Information About the p3rpc Utility" section in the "Command-Line Utilities" appendix of Cisco Service Control Management Suite Subscriber Manager User Guide.

Note PRPC authentication from the Cisco SCA BB Console to any CM/SM/Cisco SCE IP addresses other than the real IP address of the device is not supported. This is especially important when the CM/Subscriber Manager/Cisco SCE resides on the inside interface of a NATing router or firewall Workaround : Redesign your network so that the SCA BB Console is given the real IP address of the CM/SM/Cisco SCE. Disable PRPC authentication on the Cisco SCE/CM/Subscriber Manager as described in the following sections.

Introduction to Disabling PRPC Authentication

Disabling PRPC Authentication on a Cisco SCE Platform

Procedure

Use the CLI to disable PRPC authentication.
Run the **ip rpc-adapter security-level none** CLI in config mode.

Disabling PRPC Authentication on a CM

Procedure

Step 1 Edit the CM configuration file.
Edit the cm/um/config/p3cm.cfg configuration file:

```
[RPC.Server] security_level=none
```

Step 2 Reload the CM process.

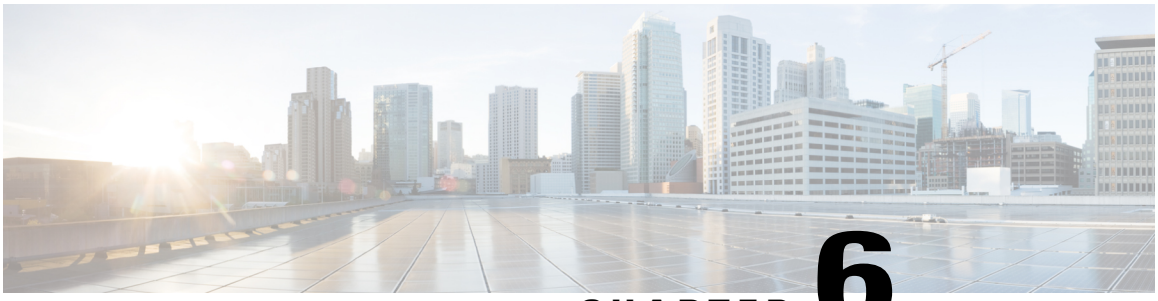
Disabling PRPC Authentication on an Subscriber Manager

Procedure

Step 1 Edit the Subscriber Manager configuration file.
Edit the ~pcube/sm/server/root/config/p3sm.cfg configuration file:

```
[RPC.Server] security_level= none
```

Step 2 Load the configuration.
Run the following CLU: **p3sm --load-config**



CHAPTER 6

Using the Service Configuration Editor

To configure a Cisco Service Control Engine (Cisco SCE) platform to handle traffic, you must define a service configuration and apply it to the platform. Use the Service Configuration Editor tool to create, define, and manage service configurations.

This module describes how to use the Service Configuration Editor tool.

- Service Configurations , page 141
- Managing Service Configurations , page 141

Service Configurations

A service configuration is a data structure that defines how the Cisco SCE platform analyses network traffic, what rules apply to the traffic, and what actions the Cisco SCE platform takes to enforce these rules.

A service configuration consists of the following two main elements:

- Services—Define the categories to which transactions are classified
- Packages—Define how the Cisco SCE platform acts upon transactions from different services

Service configurations are stored as PQB files.

Managing Service Configurations

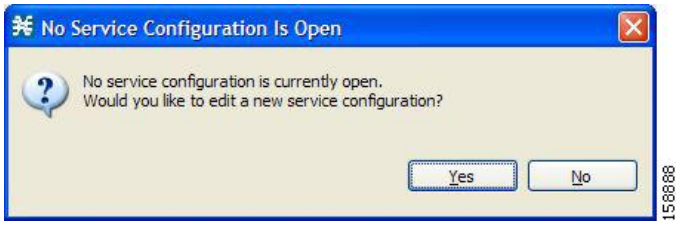
This section explains how to:

- Manage service configurations
- Export and import service configuration data
- Apply service configurations to Cisco SCE platforms and retrieve them

Opening the Service Configuration Editor Tool

If no service configurations are open when you open or switch to the Service Configuration Editor tool, a No Service Configuration Is Open dialog box appears.

Figure 90: No Service Configuration Is Open



Procedure

Step 1 To create a new service configuration (see Adding New Service Configurations , on page 142), click **Yes**.

Step 2 To open an existing service configuration (see Opening Existing Service Configurations , on page 144), click **No**.

The Configuration option is included in the main menu only when at least one service configuration is open.

You can have many service configurations open at a time; each is displayed in its own view, and you click a view to make the service configuration of the view active.

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

Adding New Service Configurations

You can add a new service configuration whenever necessary.

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

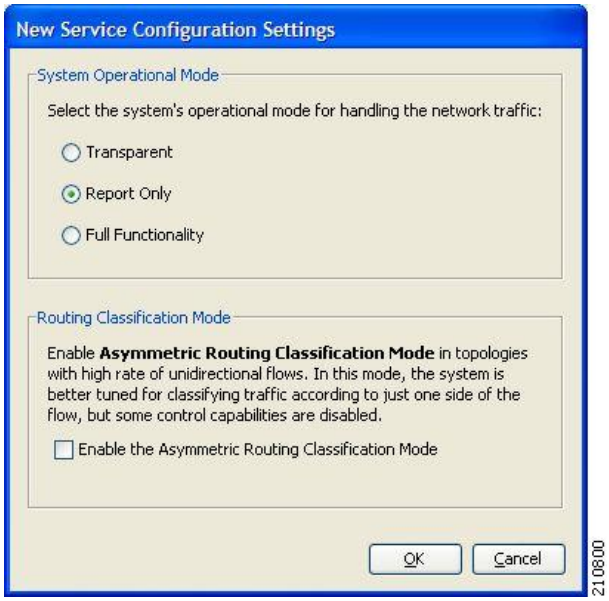
When a new service configuration opens, it contains the default service configuration supplied with SCA BB. This includes a default package, which contains a default service rule.

Procedure

Step 1 In the Console toolbar, click (New Service Configuration).

A New Service Configuration Settings dialog box appears.

Figure 91: New Service Configuration Settings



Step 2 Select an operational mode for the service configuration.

Step 3 Select a routing classification mode for the system.
Selecting asymmetric routing classification mode gives more accurate protocol classification in topologies with a high rate of unidirectional flows. Several classification, reporting, and control features are not supported when this mode is enabled (see Asymmetric Routing Classification Mode , on page 434

Step 4 Click OK.
If you have set a default DSS file, a Default Signature message appears.

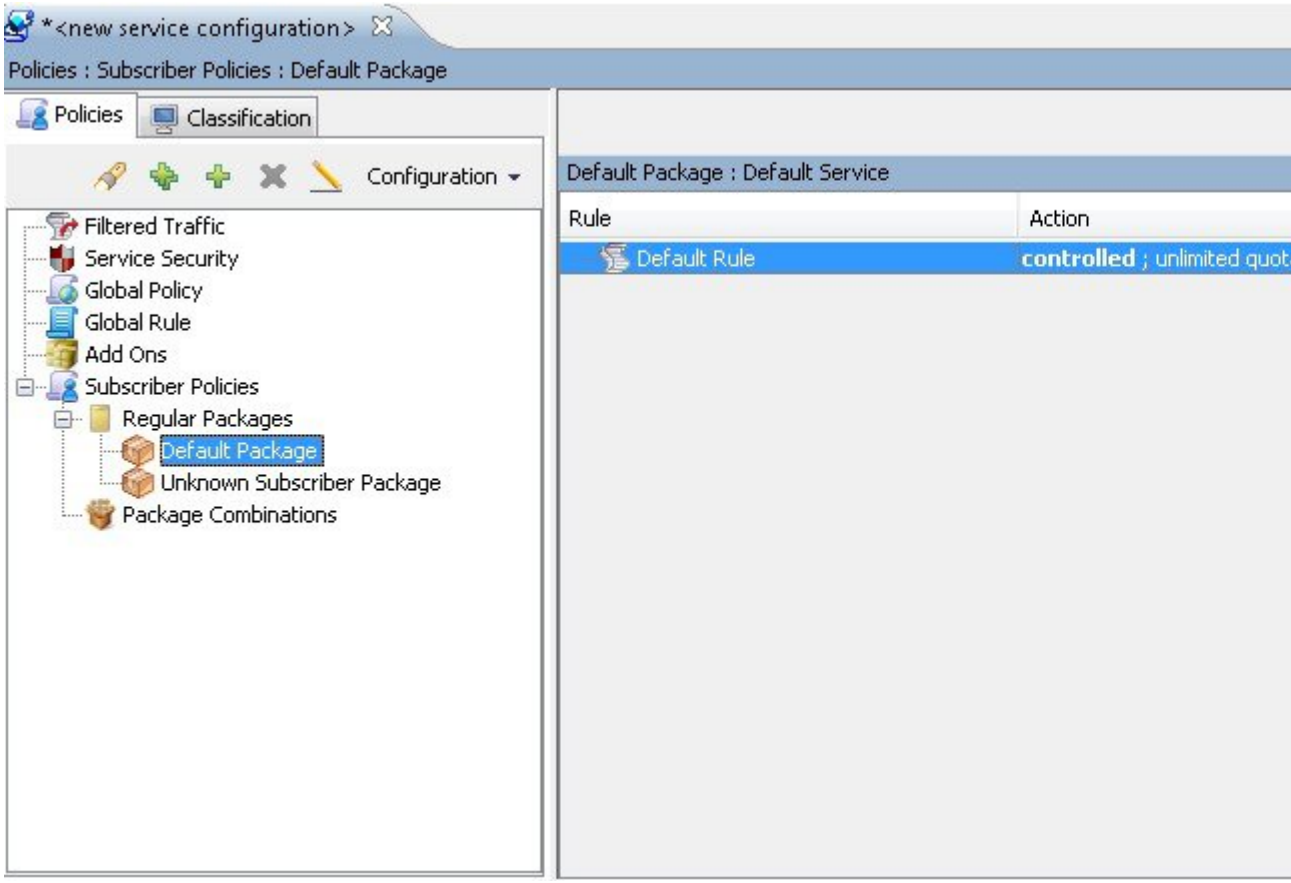
Figure 92: Default Signature



Step 5 (Recommended) Click Yes to import the default DSS file. Click No to continue without importing the default DSS file.

The new service configuration is added to the Console window, open on the Network Traffic tab, and becomes the active service configuration.

Figure 93: Service Configuration Editor



Opening Existing Service Configurations

You can open a saved service configuration for viewing or for editing, or to apply it to a Cisco SCE platform.

Service configuration files have the extension PQB.

Procedure

Step 1 In the Console toolbar, click the Open A Service Configuration File ( ) icon. Alternatively, you can choose File > Open Service Configuration from the Console main menu.
An Open dialog box appears.

Step 2 Browse to a service configuration file.

Step 3 Click Open.
The Open dialog box closes.

If the default DSS file has not been imported into the service configuration, a Default Signature message appears.

Figure 94: Default Signature



Step 4 (Recommended) Click Yes to import the default DSS file. Click No to continue without importing the default DSS file.
The service configuration is loaded into the Console. This service configuration becomes the active service configuration. The title of the Console window includes the name of the service configuration.

Note Common SCABB console is going to be used for SCE 8000 platform releases.

SCE 8000 platform level service tree will be maintained if we open 4.1.x, 5.1.x or any earlier release PQB file in 5.2.0 SCABB console.

How to Save the Current Service Configuration

You can save the active service configuration.

Saving the Current Service Configuration to a Service Configuration File

Procedure

Step 1 From the Console main menu, choose File > Save As .
A Save As dialog box appears.

Step 2 If prompted, enter your password.

Step 3 Browse to the folder where you want to save the file containing the service configuration.

Step 4 In the File name field, enter a new file name, or select an existing PQB file.

Step 5 Click Save.
During processing, a Saving Service Configuration File message appears.

The service configuration is saved to the selected file. If the file exists, it is overwritten.

Saving the Current Service Configuration to the File from Which it Was Loaded

Procedure

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

Closing Service Configurations

Procedure

Step 1 On the service configuration view, click the Close ( ) icon.
If there are no unsaved changes, the service configuration view closes. If there are unsaved changes a Save Resource message appears.

Figure 95: Save Resource



Step 2 Click Yes.

- If this is an existing edited service configuration, the changes are saved and the service configuration view closes.
- If this is a new service configuration, a Save As dialog box opens.

Step 3 Enter a name for the service configuration and click Save.
The Save As dialog box closes, the changes are saved, and the service configuration view closes.

Exporting Service Configuration Data

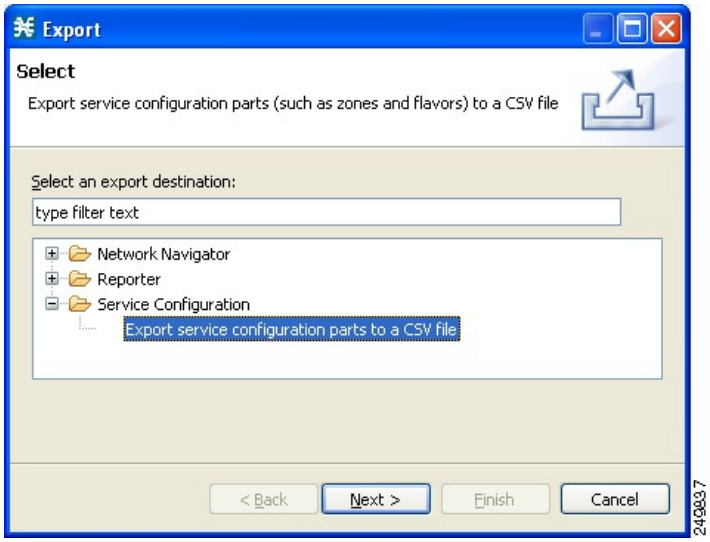
You can export service configuration data from the current service configuration to CSV files. The CSV file formats are described in the "CSV File Formats" chapter of *Cisco Service Control Application Suit for Broadband Reference Guide.*

Each type of service configuration element is exported to a separate file.

Procedure

Step 1 From the Console main menu, choose **File > Export**.
The Export dialog box appears.

Figure 96: Export

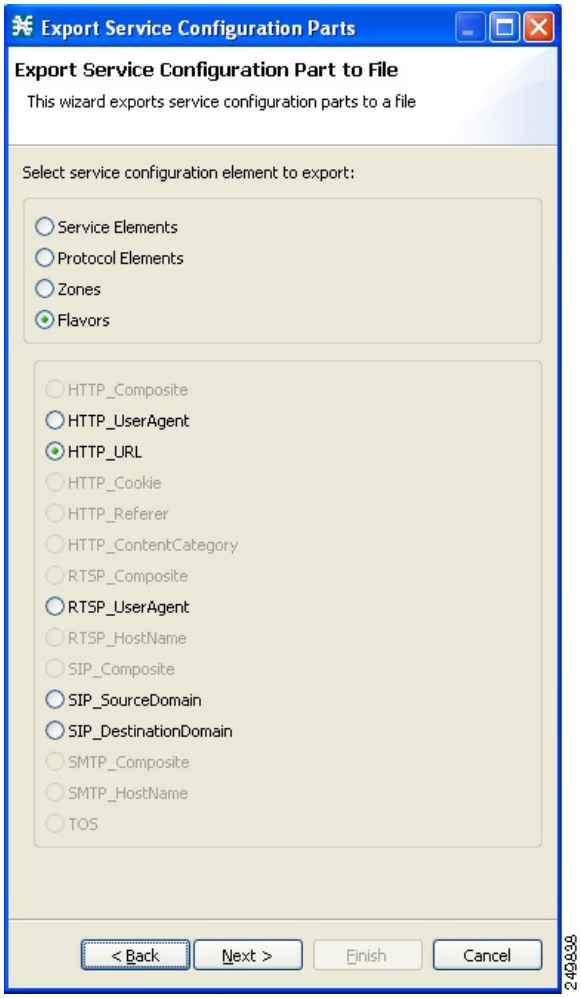


Step 2 From the export destination list, select Export service configuration parts to CSV file .

Step 3 Click **Next**.

The Export Service Configuration Parts dialog box appears.

Figure 97: Export Service Configuration Parts to File



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

- Service Elements
- Protocol Elements
- Zones
- Flavors

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

If you select Zones or Flavors, you have a choice to export the data in Standard format or Easy format.

In Easy format for flavor CSV files, lines in the files are in single URL format. for example, http://*.cisco.com/files*. Similarly, in Easy format for zone CSV files, lines in the files contains only zone items. For example, 1.0.0.0/32.

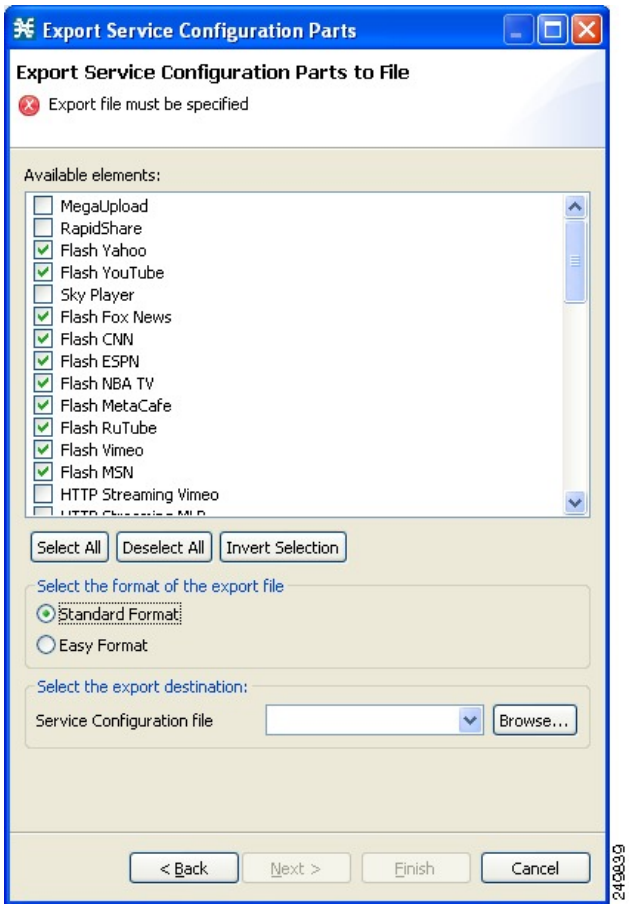
For more details on Standard format and Easy format, see the *Cisco Service Control Application for Broadband Reference Guide*.

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

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

Step 6 Click **Next**.
The second screen of the Export Service Configuration Parts dialog box opens.

Figure 98: Export Service Configuration Parts to File



The Available elements pane lists all elements in the service configuration of the selected type.

Step 7 Select the elements to export, using the check boxes and the select buttons.

Step 8 (Only for Zones and Flavors) Select the format of the export file.

Step 9 In the Select the export destination area, click **Browse**.
An Open dialog box appears.

Step 10 Browse to the folder where you want to save the file containing the service configuration elements.

Step 11 In the File name field, enter a new file name, or select an existing CSV file.
(Only for Zones and Flavors) For Easy format, you must select the folder and the file name is the Zone or Flavor name.

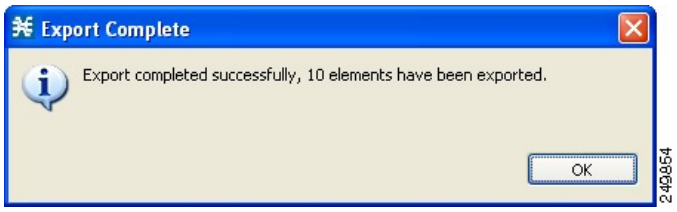
Step 12 Click **Open** to select the file.
If the file exists, it is overwritten.

The Open dialog box closes.

Step 13 Click Finish.
The selected service configuration elements are exported to the file.

An Export Complete message appears.

Figure 99: Export Complete



Step 14 Click **OK**.
The Export Service Configuration Parts dialog box closes.

Importing Service Configuration Data

You can import service configuration data to the current service configuration from CSV files. The CSV file formats are described in the "CSV File Formats" chapter of Cisco Service Control Application Suit for Broadband Reference Guide.

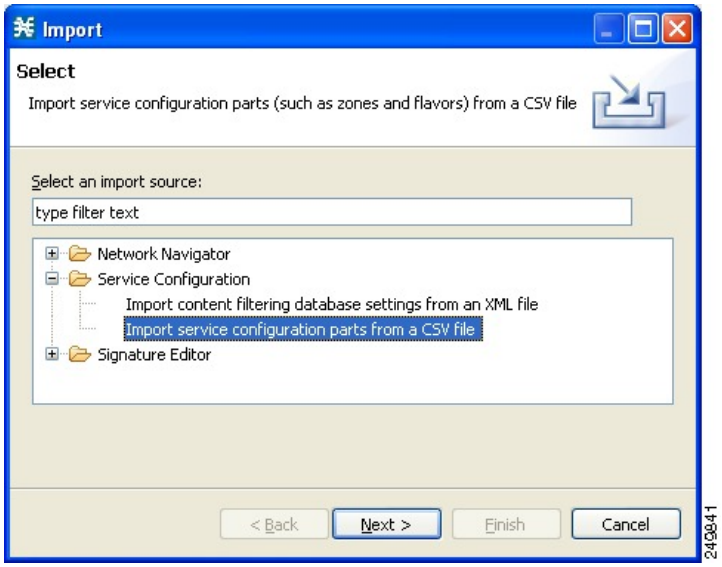
Each type of service configuration element is imported from a separate file.

Procedure

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

The Import dialog box appears.

Figure 100: Import



Step 2 From the Select an import source list, select Import service configuration parts from CSV file .

Step 3 Click Next.

The Import Service Configuration Parts dialog box appears.

Figure 101: Import Service Configuration Parts from File



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

- Service Elements
- Protocol Elements
- Zones
- Flavors

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

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

Step 6 Click Next .

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

Figure 102: Import Service Configuration Parts from File



Step 7 (Only for Zones and Flavors) Select the format to Import.

Step 8 Click Browse.
An Open dialog box appears.

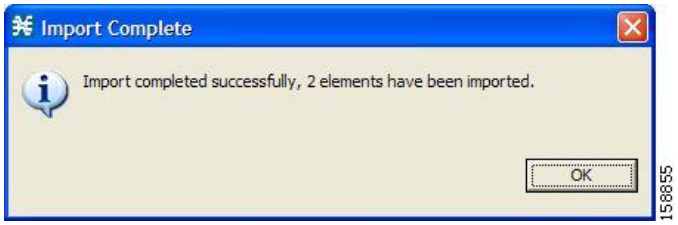
Step 9 Browse to the folder containing the file to import, and select a CSV file.

Step 10 Click Open to select the file.
The Open dialog box closes.

Step 11 Click Finish.
The configuration elements are imported from the file.

An Import Complete message appears.

Figure 103: Import Complete



Step 12 Click OK.
The Import Service Configuration Parts dialog box closes.

How to Apply and Retrieve Service Configurations

For a new or edited service configuration to take effect, you must apply it to the Cisco SCE platform. Until you do, the Cisco SCE platform continues to enforce the previous service configuration.

You can use the Service Configuration Editor to apply a service configuration to a Cisco SCE platform, but not to retrieve a service configuration.

You can apply or retrieve a service configuration using:

- The Network Navigator Tool , on page 107
- **servconf,** the Cisco SCA BB Service Configuration Utility (see The Cisco SCA BB Service Configuration Utility , on page 509)

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 in the service configuration.

The Validate process runs automatically when you select Apply Service Configuration to SCE devices. The Validation Results dialog box appears only if the procedure found errors or issued warnings about the current service configuration.

Procedure

Step 1 From the Console main menu, choose File > Validate .
The Validation Results dialog box appears.

Figure 104: Validation Results - Service Configuration is valid

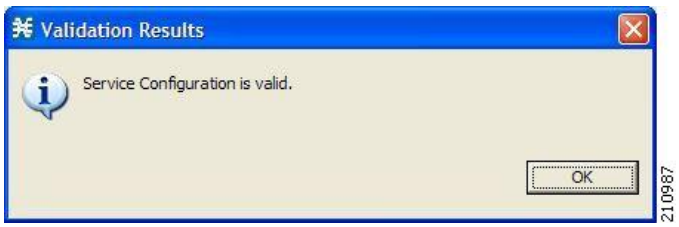
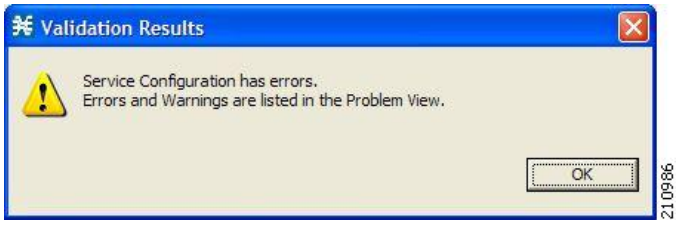


Figure 105: Validation Results - Service Configuration has errors



Any problems with the service configuration are listed in the Problems view.

Step 2 Click OK.
The Service Configuration Validation dialog box closes.

Applying a Service Configuration to SCE Platforms

When you click Apply Service Configuration to SCE Devices, the validation process runs automatically on the current service configuration.

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

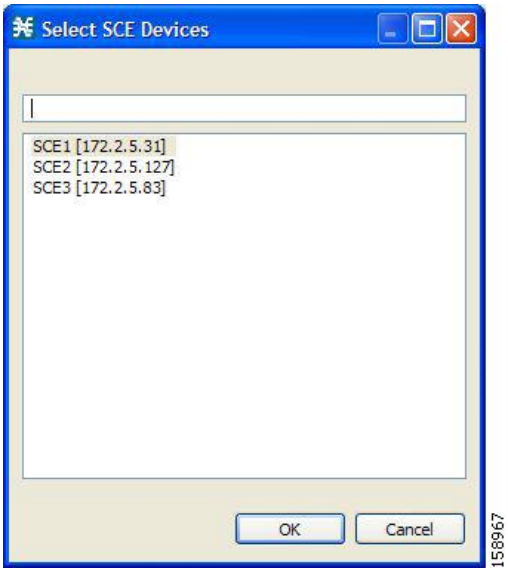
Note If anomaly-based detection of malicious traffic is enabled, any access control list (ACL) that is configured on the Service Control Engine (SCE) platform but is not applied to anything (for example, an interface, an access map, or an SNMP community string) might be deleted when a service configuration is applied to the platform. Workaround : Disable anomaly-based detection of malicious traffic. In the Network Traffic tab, select Service Security . In the Service Security Dashboard, clear the Enable anomaly detection check box.

Procedure

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

The Select SCE Devices dialog box appears.

Figure 106: Select SCE Devices



All SCE platforms defined in the Network Navigator are listed in the dialog box.

Step 2 Select one or more SCE platforms from the list.

Step 3 Click OK.
A Password Management dialog box appears for each platform selected.

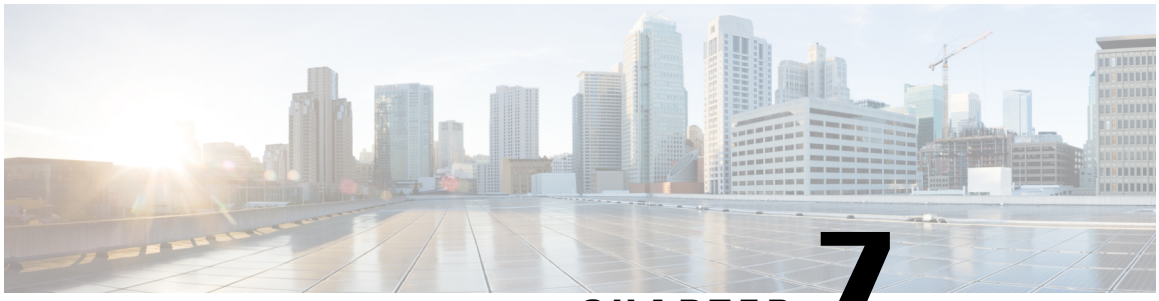
Step 4 Enter the appropriate password.

Step 5 Click **Apply**.
The Password Management dialog box closes.

An Applying service configuration to SCE progress bar appears for each SCE platform selected.

The validation process runs on the service configuration.

- If there is a problem and the validation process ends with a warning or error, the Validation Results dialog box appears. Click OK, modify the service configuration based on the information provided in the Problems view, and then repeat this procedure.
- If the validation process runs successfully, the service configuration is applied to the selected SCE platforms.



CHAPTER 7

TrafficClassificationUsingServiceConfiguration Editor

Traffic classification is the first step in creating a Cisco SCA BB service configuration. Traffic is classified according to services.

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

This module explains how to work with services and their elements and subelements:

- Searching Traffic Classification Settings, page 157
- Introduction to Managing Services , page 158
- Introduction to Managing Protocols , page 177
- Introduction to Managing Zones, page 189
- Introduction to Managing Protocol Signatures , page 200
- Introduction to Managing Flavors , page 213
- Introduction to Managing Content Filtering, page 228
- OS Fingerprinting Overview, page 243
- Configuring Policy for DNS Assisted Classification, page 247

Searching Traffic Classification Settings

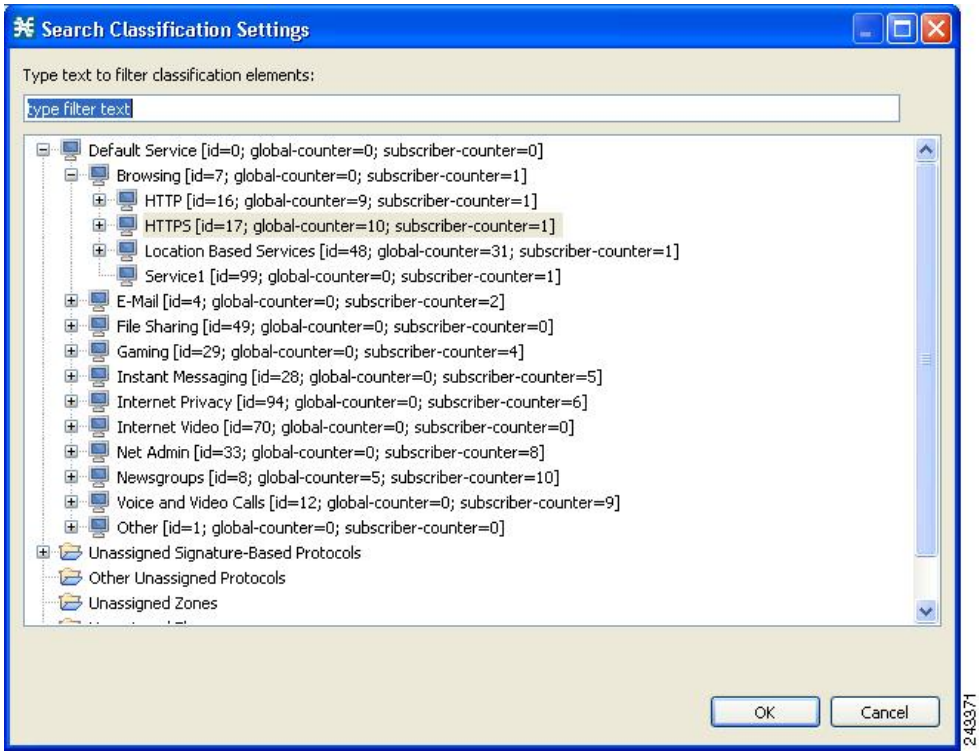
You can search for any classification detail by name or numeric ID, such as services, protocols, port number, or counter assignments. You can also search for protocols or signatures that are not assigned to a service.

Procedure

Step 1 In the Classification tab, click the Search Classification Settings () icon.

The Search Classification Settings dialog box appears.

Figure 107: Search Classification Settings



Step 2 Enter the text to search.
You can include the following wildcards in the search:

- ?—any character
- *—any string

The dialog box is populated with the search results.

Step 3 Double-click the item to take you to the screen where you can edit it.

Example:
For example, if you double-click a protocol, the protocol dialog box opens on the selected protocol.

Introduction to Managing Services

Services are used to classify controlled traffic.

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

Traffic is classified based on some or all of the following:

- Protocol—The protocol used by the transaction, as identified by the Cisco Service Control Engine (Cisco SCE) platform
- Initiating side—Where the transaction was initiated
- Zone—IP address of the network-side host of the transaction
- Flavor—Specific Layer 7 properties of the transaction; for example, host names of the network-side host of the transaction

A service configuration can contain up to 500 services and 10,000 service elements. Every service element in a service configuration must be unique.

Service Parameters

A service is defined by the following parameters:

- General parameters:
  - Name—A unique name
  - Description—(Optional) A description of the service
- Hierarchy parameters:
  - Parent Service
    The default service, which is the base of the service hierarchy, does not have a parent.

    Note The parent service is important when services share usage counters (see next parameter).
  - Service Usage Counters—Used by the system to generate data about the total use of each service. A service can use either its own usage counters, or those of the parent service.
    Each usage counter has:
    - A name assigned by the system (based on the service name).

      Note An asterisk is appended to a service usage counter name whenever the counter applies to more than one service.
    - A unique counter index—A default value of the counter index provided by the system. Do not modify this value.
- Advanced parameter:
  - Service Index—A unique number by which the system recognizes the service (changing the service name does not affect Cisco SCE platform activity). The system provides a default value of the service index. Do not modify this value.

These parameters are defined when you add a new service (see Adding a Service to a Service Configuration , on page 160 section). You can modify them at any time (see Editing Services , on page 165 section).

How to Add and Define Services

A number of services are predefined in the Console installation. You can add additional services to a service configuration, subject to the limit of 500 services (including predefined services) per service configuration.

After you have added and defined a new service, you can add service elements to the service (see the Adding Service Elements section).

This section contains the following topics:

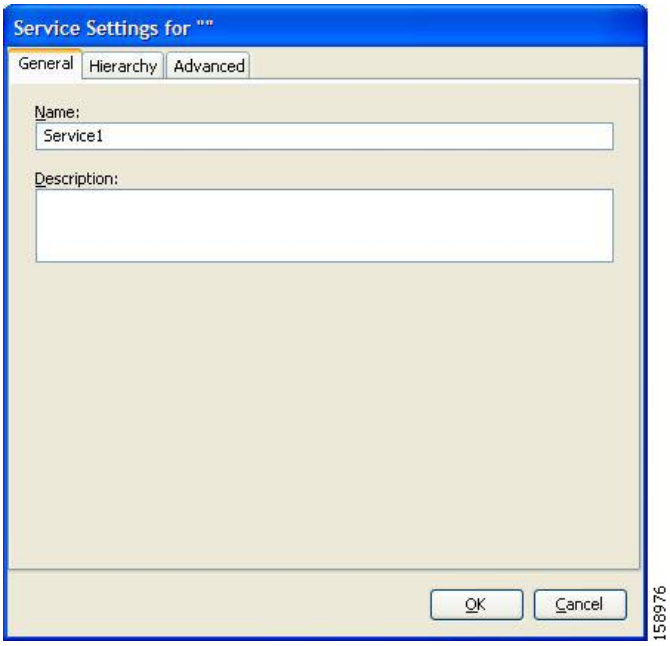
Adding a Service to a Service Configuration

Procedure

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

Step 2 In the left pane, click the Add Service ( ) icon.
The Service Settings dialog box appears.

Figure 108: Service Settings



Step 3 In the Name field, enter a unique and relevant name for the service.

Step 4 In the Description field, enter a meaningful and useful description of the service.

Step 5 To set exclusive usage counters for this service, or to change the parent service you selected when adding the service, continue with the instructions in the Defining Hierarchical Settings for a Service , on page 161 section.

Step 6 (Optional) To specify an index for this service, continue with the instructions in the Setting the Service Index , on page 162 section.

Note The system automatically assigns a free number for the new service. Modify this number only where a specific index value must be assigned to a specific service.

Step 7 Click **OK**.
The Service Settings dialog box closes.

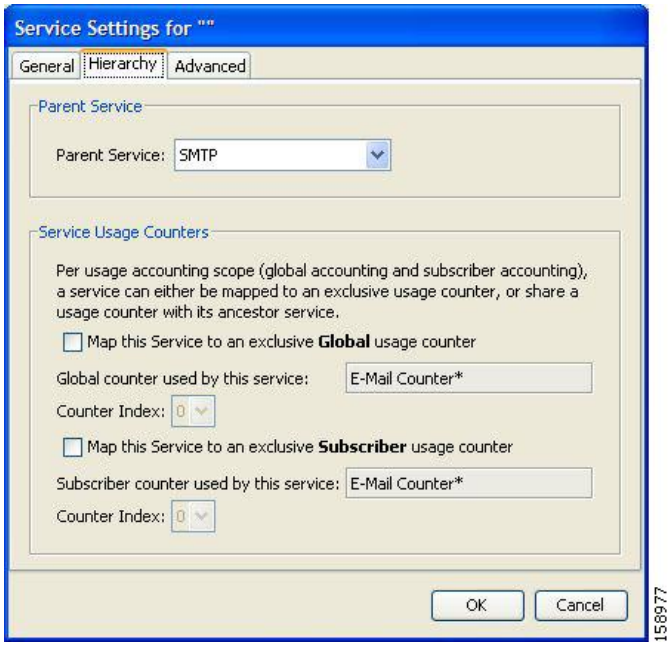
The service is added to the service tree as a child to the service you selected in the hierarchy.

Defining Hierarchical Settings for a Service

Procedure

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

Figure 109: Hierarchy Tab



Step 2 To set a different parent service, select the desired parent from the **Parent Service** drop-down list.

Step 3 By default, a new service uses the global usage counter of its parent service. To define an exclusive global usage counter, check the **Map this Service to an exclusive Global usage counter** check box.
The name in the read-only Global counter of this service field changes to reflect your choice.

The **Counter Index** drop-down list is enabled.

(Optional) Select a value for the counter index from the **Counter Index** drop-down list. You can select upto counter index values.

Note The system provides a default value of the counter index. Do not modify this value.

Step 4 By default, a new service uses the subscriber usage counter of its parent service. To define an exclusive subscriber usage counter, check the **Map this Service to an exclusive Subscriber usage counter** check box. The name in the read-only Subscriber counter of this service field changes to reflect your choice.

The **Counter Index** drop-down list is enabled.

(Optional) Select a value for the counter index from the **Counter Index** drop-down list. You can select upto counter index values.

Note The system provides a default value of the counter index. Do not modify this value.

Step 5 To specify an index for this service, continue with the instructions in the Setting the Service Index , on page 162 section.

Note The system automatically assigns a free number for the new service. Modify this number only where a specific index value must be assigned to a specific service.

Step 6 Click **OK**.
The Service Settings dialog box closes.

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

Setting the Service Index

Procedure

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

The Advanced tab opens.

Figure 110: Advanced Tab



Step 2 From the Set the Index for this Service drop-down list, select a service index.
The service index must be an integer in the range from 1 to 499; zero is reserved for the default service.

Note The system automatically assigns a free number for the new service. Modify this number only where a specific index value must be assigned to a specific service.

Step 3 Click OK.
The Service Settings dialog box closes.

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

Viewing Services

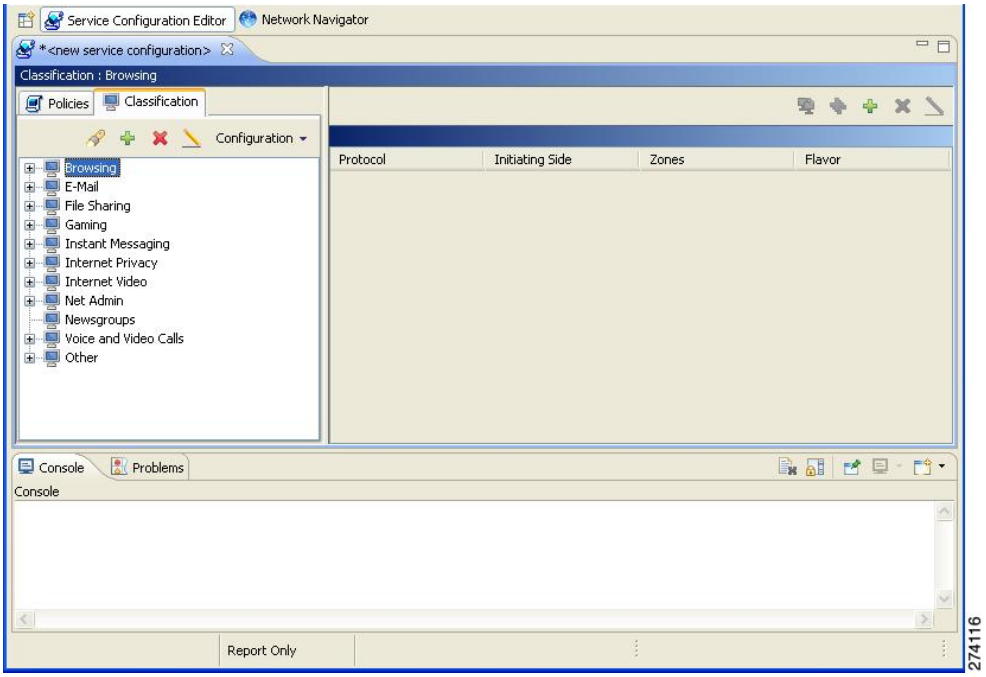
You can view a hierarchy tree of all existing services and see their associated service elements.

Procedure

Step 1 In the current service configuration, click the Classification tab.

The Classification tab appears.

Figure 111: Classification Tab

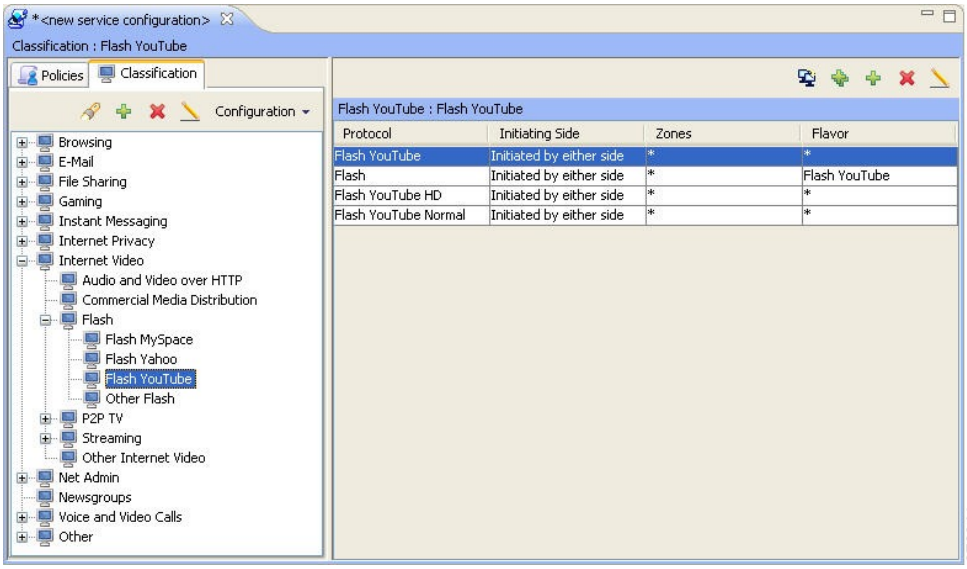


A list of all services is displayed in the service tree (left pane).

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

A list of all service elements defined for this service is displayed in the right (Service Elements) pane.

Figure 112: Service Elements



Step 3 To view more information about a service, select a service from the service tree and click the Edit Service () icon.
The Service Settings dialog box appears.

Step 4 Click OK.
The Service Settings dialog box closes.

Editing Services

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

To add, modify, or delete service elements, see Introduction to Managing Service Elements , on page 167 section.

Procedure

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

Step 2 In the left pane, click the Edit Service () icon.
The Service Settings dialog box appears.

Step 3 (Optional) Give a new name to the service.
Enter a new name in the Name field.

Step 4 (Optional) Give a new description for the service.

Enter a new description in the Description field.

Step 5 To change hierarchical settings, click the Hierarchy tab.
The Hierarchy tab opens.

Step 6 To set a different parent service, select the desired service from the Parent Service drop-down list.

Step 7 To share a global usage counter with the parent service, uncheck the Map this Service to an exclusive Global usage counter check box.
The name of the parent service's counter is displayed in the Global counter used by this service field.

Step 8 To define an exclusive global usage counter, check the **Map this Service to an exclusive Global usage counter** check box.
The name in the read-only Global counter of this service field changes to reflect your choice.

The Counter Index drop-down list is enabled.

Note The system provides a default value of the counter index. Do not modify this value.

Step 9 To share a subscriber usage counter with the parent service, uncheck the **Map this Service to an exclusive Subscriber usage counter** check box.
The name of the parent service's counter is displayed in the Subscriber counter used by this service field.

Step 10 To define an exclusive subscriber usage counter, check the Map this Service to an exclusive Subscriber usage counter check box.
The name in the read-only Subscriber counter of this service field changes to reflect your choice.

The Counter Index drop-down list is enabled.

Note The system provides a default value of the counter index. Do not modify this value.

Step 11 Change the service index. To change the service index:

a) In the Service Settings dialog box, click the Advanced tab.
b) The Advanced tab opens.

Step 12 From the Set the Index for this Service drop-down list, select a service index.
The service index must an integer in the range from 1 to 499; zero is reserved for the default service.

Note The system provides a default value of the service index. Do not modify this value.

Step 13 Click OK .
The Service Settings dialog box closes.

The changes to the service are saved.

Deleting Services

You can delete all services, even those services in the Console installation, except for the default service.

Procedure

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

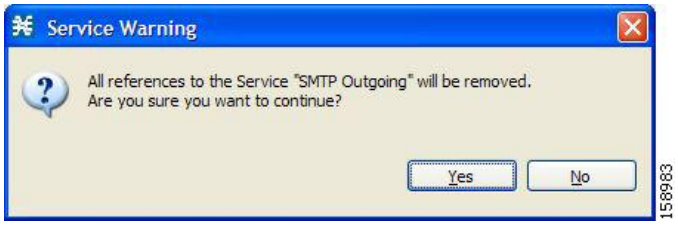
Step 2 In the left pane, click the Delete Service ( ) icon.
A Service Warning message appears.

Figure 113: Service Warning



Step 3 Click Yes.
If any package has a rule for this service (see Introduction to Managing Rules, on page 331 section), a second Service Warning message appears.

Figure 114: Service Warning



Step 4 Click Yes.
The service is deleted and is no longer displayed in the service tree. Any rules for the service are also deleted.

Children of the deleted service are not deleted; they move up one level in the service tree.

Introduction to Managing Service Elements

A service is a collection of service elements; to complete the definition of a service, you must define its service elements. A service element maps a specific protocol, initiating side, zone, and flavor to the selected service.

For more information, see Introduction to Managing Protocols , on page 177 section , Introduction to Managing Zones, on page 189 section , and Introduction to Managing Flavors , on page 213 section .

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

A service element maps a traffic flow, that meets all the following criteria, to its service:

- The flow uses the specified protocol of the service element.
- The flow is initiated by the side (network, subscriber, or either) specified for the service element.
- The destination of the flow is an address that belongs to the specified zone of the service element.

- The flow matches the specified flavor of the service element.
- The service element is the most specific service element satisfying the first four criteria.

Adding Service Elements

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

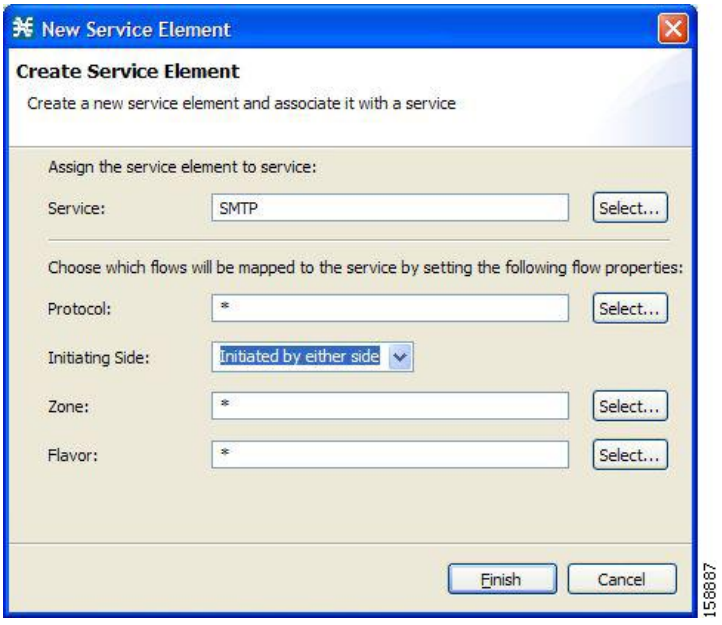
Note Every service element must be unique. If, at any stage, the new service element is the same as an existing one, an error message is displayed in the dialog box, and the Finish button is dimmed. To proceed, modify the value in at least one field.

Procedure

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

Step 2 In the right (Service Elements) pane, click the **Add Service Element** ( ).
The New Service Element dialog box appears.

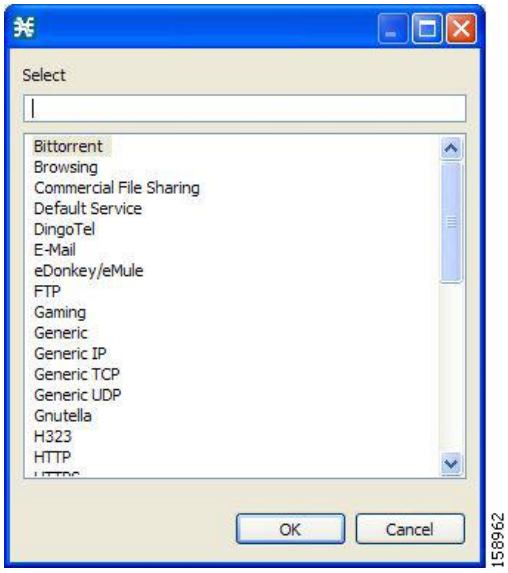
Figure 115: New Service Element



Step 3 To change the service to which this service element is assigned, click the Select button next to the Service field.

The Select a Service dialog box appears, displaying a list of all services.

Figure 116: Select a Service



Step 4 Select a service from the list.

Step 5 Click **OK**.
The Select a Service dialog box closes.

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

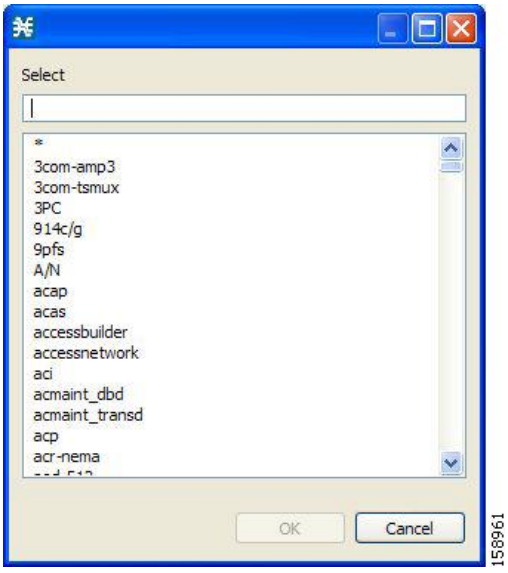
Step 6 Click the Select button next to the Protocol field.

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

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

Note If you select a flavor (Step 15) before you select a protocol, only protocols relevant to the selected flavor are displayed.

Figure 117: Select a Protocol



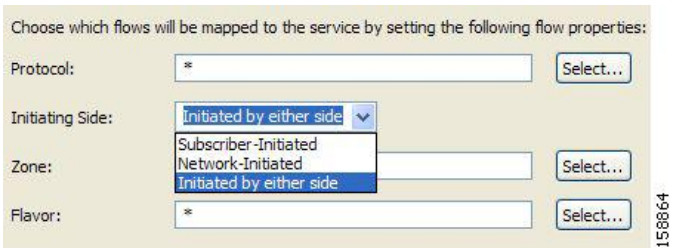
Step 7 Select a protocol from the list. You can type in the field at the top of the dialog box to help locate the desired protocol.

Step 8 Click **OK**.
The Select a Protocol dialog box closes.

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

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

Figure 118: Initiating Side Field



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

- Subscriber-Initiated —Transactions are initiated at the subscriber side towards (a server at) the network side.
- Network-Initiated —Transactions are initiated at the network side towards (a server at) the subscriber side.

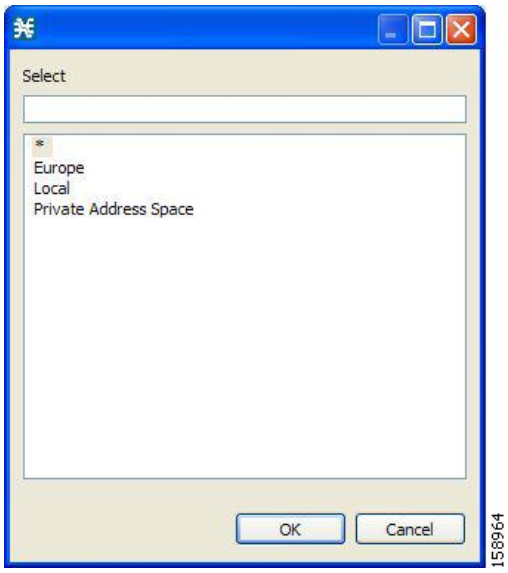
- Initiated by either side.

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

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

The Select a Zone dialog box appears (Figure 7-13), displaying a list of all zones.

Figure 119: Select a Zone



Step 12 Select a zone from the list.

Step 13 Click **OK**.

The Select a Zone dialog box closes.

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

Note If you select a zone in which data flows are classified using zones only, the Protocol, Initiating Side, and Flavor fields are disabled.

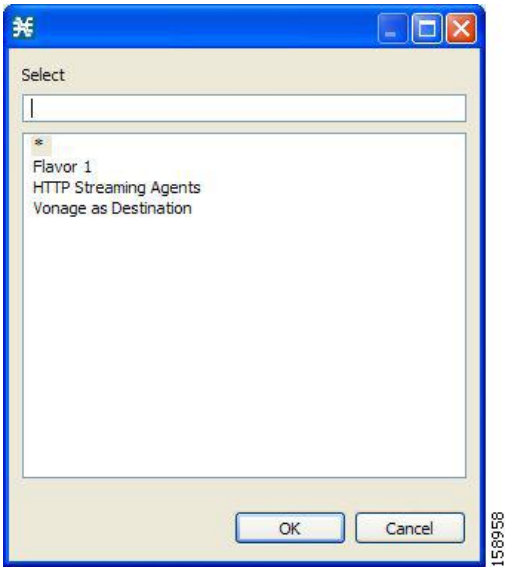
Step 14 Click the Select button next to the Flavor field.

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

The Select a Flavor dialog box appears, displaying a list of all flavors relevant to the protocol selected in Step 7.

Note You can only select a ToS flavor if you select the default value (*, meaning any protocol) for the protocol.

Figure 120: Select a Flavor



Step 15 Select a flavor from the list.

Step 16 Click **OK**.
The Select a Flavor dialog box closes.

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

Step 17 Click **Finish**.
The New Service Element dialog box closes.

The new service element is added to the service.

A new row, representing the service element, is added to the service element list in the Service Elements pane.

Duplicating Service Elements

Duplicating an existing service element is a useful way to add a new service element similar to an existing service element. It is faster to duplicate a service element and then modify it than to define the service element from beginning.

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

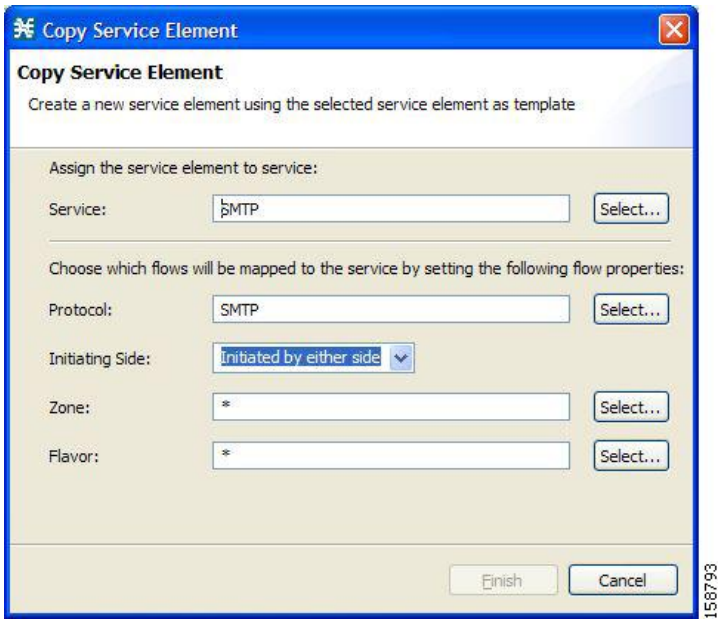
Procedure

Step 1 In the Services tab, select a service from the service tree.
A list of associated service elements is displayed in the Service Elements pane.

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

Step 3 Click the Duplicate Service Element ( ) icon.
The Copy Service Element dialog box appears.

Figure 121: Copy Service Element



Step 4 Modify the service element
(see Editing Service Elements , on page 173 section).

Note Before you can save the new service element, you must change the value in at least one field.

Editing Service Elements

You can modify all service elements, even those service elements that are included in the Console installation.

Note Every service element must be unique. If, at any stage, the modified service element is the same as an existing one, an error message is displayed in the dialog box, and the Finish button is dimmed. To proceed, modify the value in at least one field.

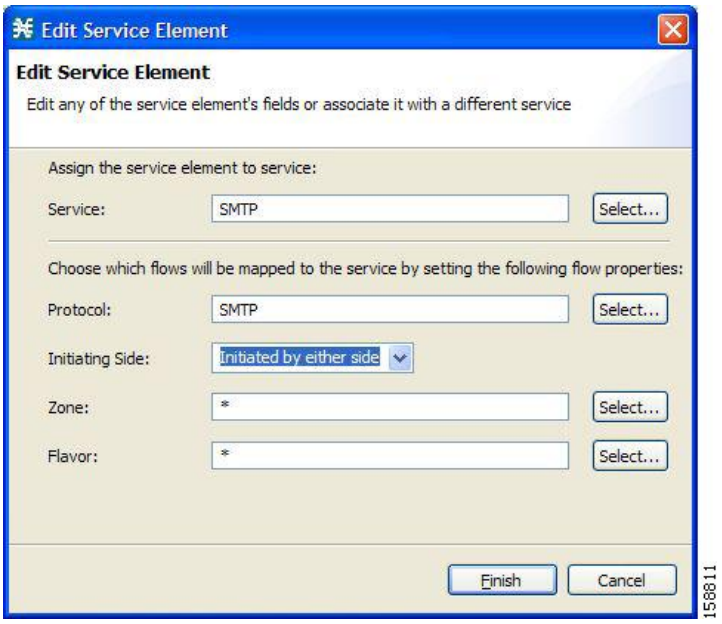
Procedure

Step 1 In the Services tab, select a service from the service tree.
A list of associated service elements is displayed in the Service Elements pane.

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

Step 3 In the Service Elements pane, click the Edit Service Element ( ) icon.
The Edit Service Element dialog box appears.

Figure 122: Edit Service Element



Step 4 To change the service to which this service element is assigned, click the Select button next to the Service field.
The Select a Service dialog box appears, displaying a list of all services.

Step 5 Select a service from the list.

Step 6 Click OK.
The Select a Service dialog box closes.

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

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

Note An asterisk (*) means that no protocol checking is performed when testing whether a flow maps to this service element.

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

Step 8 Select a protocol from the list; you can type in the field at the top of the dialog box to help locate the desired protocol.

Step 9 Click OK.
The Select a Protocol dialog box closes.

The selected protocol is displayed in the Protocol field of the Edit Service Element dialog box.

Step 10 To change the initiating side of this service element, click the drop-down arrow in the Initiating Side field.

Step 11 Select the appropriate initiating side from the drop-down list.

- Subscriber-Initiated —Transactions are initiated at the subscriber side towards (a server at) the network side.
- Network-Initiated —Transactions are initiated at the network side towards (a server at) the subscriber side.
- Initiated by either side

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

Note An asterisk (*) means that no zone checking is performed when testing whether a flow maps to this service element.

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

Step 13 Select a zone from the list.

Step 14 Click OK.

The Select a Zone dialog box closes.

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

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

Note An asterisk (*) means that no flavor checking is performed when testing whether a flow maps to this service element.

The Select a Flavor dialog box appears, displaying a list of all flavors.

Step 16 Select a flavor from the list.

Step 17 Click OK.

The Select a Flavor dialog box closes.

The selected flavor is displayed in the Flavor field of the Edit Service Element dialog box.

Step 18 Click Finish.

The Edit Service Element dialog box closes.

The changes to the service element are saved.

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

Deleting a Service Element

You can delete all service elements, even those service elements that are included in the Console installation.

Procedure

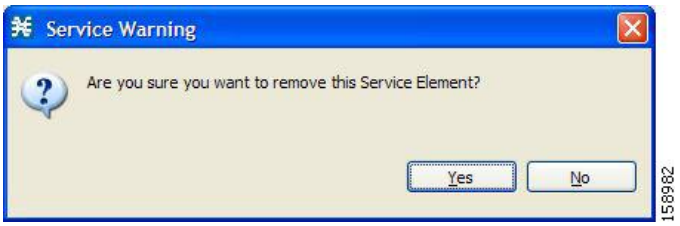
Step 1 In the Services tab, select a service from the service tree.

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

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

Step 3 In the Service Elements pane, click the Delete Service Element ( ) icon.
A Service Warning message appears.

Figure 123: Service Warning



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.

Procedure

Step 1 In the Services tab, select a service from the service tree.
A list of associated service elements is displayed in the Service Elements pane.

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

Step 3 Click the Move Service Element to Another Service ( ) icon.

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

Figure 124: Move Service Element



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.

Introduction to Managing Protocols

A protocol is composed of an application protocol signature, the destination port or ports, a unique name, and an optional description.

Protocols are used to define service elements (see the Introduction to Managing Service Elements , on page 167 section).

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

A service configuration can contain up to 10,000 protocols.

Cisco SCA BB supports many commercial and common protocols.

For a complete list of protocols included with the current release of Cisco SCA BB, see the “Information About Protocols” section in the “Default Service Configuration Reference Tables” chapter of *Cisco Service Control Application for Broadband Reference Guide.*

This section explains the following procedures:

As new protocols are released, Cisco provides files containing the new protocol signatures so that you can add the signatures to your service configuration. See the Importing a Dynamic Signature Script into a Service Configuration , on page 205.

Viewing Protocols

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

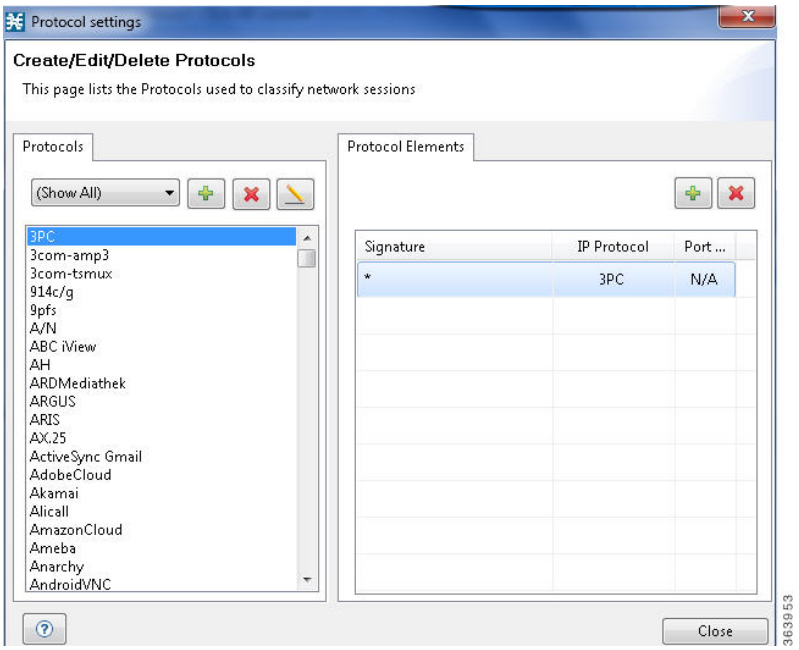
The protocols are listed in ASCII sort order (that is, 0... 9, A... Z, a... z).

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

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Protocols .
The Protocol Settings dialog box appears.

Figure 125: Protocol Settings



The Protocols tab displays a list of existing protocols.

Step 2 Double-click a protocol to view its description and ID.

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

Figure 126: Protocol Settings



Step 3 Click Cancel.
The Protocol Settings dialog box closes.

Step 4 To view a list of protocol elements, select a protocol in the list in the Protocol Settings dialog box.
Protocol elements are displayed in the Protocol Elements tab.

Step 5 Click Close .
The Protocol Settings dialog box closes.

Filtering a Protocols List

You can filter the protocols by type, so that the Protocols tab displays only the selected type of protocol.

The categories of protocols include:

- Generic Protocols—Generic IP, Generic TCP, and Generic UDP protocols, used for transactions that are not specifically mapped to a protocol by any other protocol type.
- IP Protocols—Protocols (such as ICMP), other than TCP and UDP protocols, identified according to the IP protocol number of the transaction.
- Port-Based Protocols—TCP and UDP protocols, classified according to their well-known ports. The default service configuration includes more than 750 common port-based protocols.
- Signature-Based Protocols—Protocols classified according to a Layer 7 application signature. Includes the most common protocols, such as HTTP and FTP, and a large group of popular P2P protocols.
- P2P Protocols—Peer-to-peer file-sharing application protocols, classified according to a Layer 7 application signature.
- VoIP Protocols—Voice-over-IP application protocols, classified according to a Layer 7 application signature.

- SIP Protocols—Protocols classified according to a Layer 7 application signature that is SIP or has SIP characteristics.
- Worm Protocols—Protocols classified according to a Layer 7 application signature that is based on traffic patterns of internet worms.
- Packet Stream Pattern Based Protocols—Protocols classified according to a Layer 7 application signature that is based on the pattern of the packet stream (for example, the stream's symmetry, average packet size, and rate) rather than on the payload content of the packet.
- Unidirectionally Detected Protocols—Protocols having a unidirectional signature.
- Behavioral Protocols
- E-Mail and Newsgroup Protocols
- Gaming Protocols
- HTTP Protocols
- Instant Messaging Protocols
- Net Admin Protocols
- Video Protocols
- Tunneling Protocols
- ClickStream Protocols



Note Some protocols belong to more than one category. In particular, all predefined P2P, VoIP, SIP, Worm, and Packet Stream Pattern-Based Protocols are also defined as Signature-Based Protocols.

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Protocols .
The Protocol Settings dialog box appears.

Step 2 From the drop-down list in the Protocols tab, select the type of protocol to display.
The protocols of the selected type appear in the Protocols tab.

Step 3 Click Close.
The Protocol Settings dialog box closes.

Note The setting in the drop-down list is not saved. The next time you open the Protocol Settings dialog box, all protocols are displayed.

Adding Protocols to a Service Configuration

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

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Protocols .
The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, click the Add Protocol ( ) icon.
The Protocol Settings dialog box appears.

Figure 127: Protocol Settings



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

Step 4 (Optional) From the Protocol ID drop-down list, select an ID for the protocol.
The protocol ID must be an integer in the range from 5000 to 9998; lower values are reserved for protocols provided by Cisco SCA BB.

Note The system provides the value of the protocol ID. Do not modify this field.

Step 5 Click **OK**.
The Protocol Settings dialog box closes.

The new protocol is displayed in the Protocols tab. You can now add protocol elements to it. See Adding Protocol Elements , on page 184 section.

Editing Parameters of a Protocol

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

To add, modify, or delete protocol elements, see Introduction to Managing Protocol Elements , on page 183 section.

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Protocols .
The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, double-click a protocol.
A second Protocol Settings dialog box appears.

Figure 128: Protocol Settings



Step 3 Modify fields in the Protocol Settings dialog box.

a) In the Name field, enter a new name for the protocol.

b) From the Protocol ID drop-down list, select an ID for the protocol.
The protocol ID must be an integer in the range from 5000 to 9998; lower values are reserved for protocols provided by Cisco SCA BB.

Note The system provides the protocol ID. Do not modify this field.

Step 4 Click OK.
The Protocol Settings dialog box closes.

The new values of the protocol parameters are saved.

Step 5 Click Close.
The Protocol Settings dialog box closes.

Deleting Protocols

You can delete all protocols, even those protocols that are included in the Console installation.

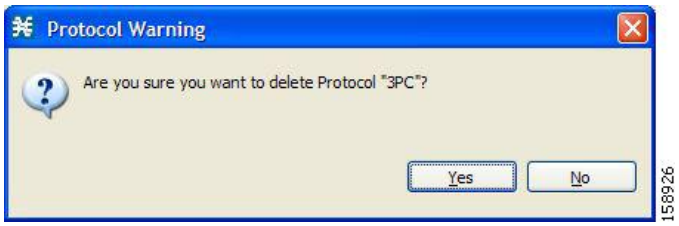
Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Protocols .
The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, select a Protocol.

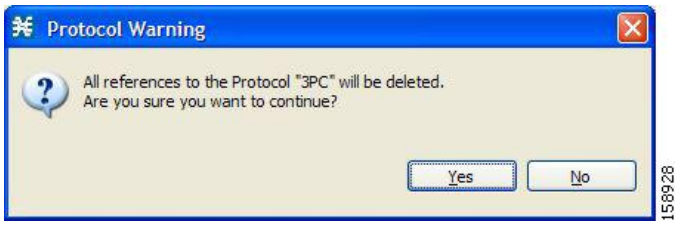
Step 3 In the Protocols tab, click the Delete Protocol ( ) icon.
A Protocol Warning message appears.

Figure 129: Protocol Warning



Step 4 Click Yes .
If any service element maps the selected protocol to a service (see Moving Service Elements , on page 176 section), a second Protocol Warning message appears (even if the service is not used by any package).

Figure 130: Protocol Warning



Step 5 Click Yes.
The Protocol is deleted from the Protocols tab.

Step 6 Click Close.
The Protocol Settings dialog box closes.

Introduction to Managing Protocol Elements

A protocol is a collection of protocol elements.

To complete the definition of a protocol, you must define its protocol elements. A protocol element maps a specific signature, IP protocol, and port range to the selected protocol. Every protocol element in a service configuration must be unique.

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

- The flow belongs to the specified signature of the protocol element.
- The flow protocol is the specified IP protocol of the protocol element.
- (If the IP protocol is TCP or UDP) The destination port is within the specified port range of the protocol element.
- The protocol element is the most specific protocol element satisfying the first three criteria.

Adding Protocol Elements

You can add any number of protocol elements to a protocol.



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

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Protocols .
The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, select a protocol.

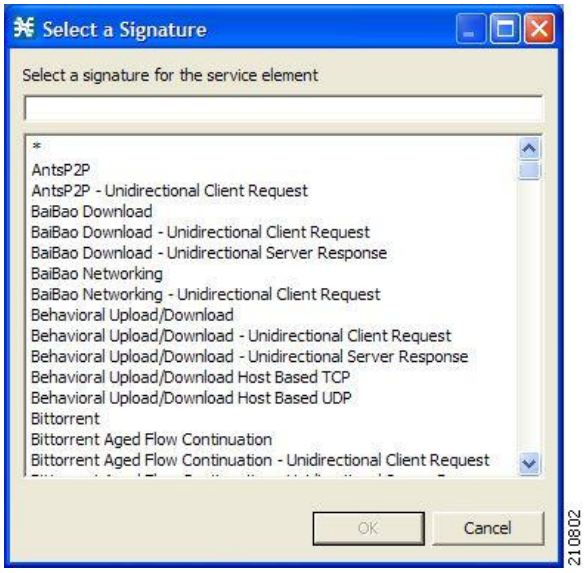
Step 3 In the Protocol Elements tab, click the Add Protocol Element () icon.
A protocol element is added to the protocol.

A new row, representing the protocol element, is added to the protocol element list in the Protocol Element tab.

Step 4 Click in the Signature cell of the protocol element, and then click the Browse button that appears in the cell.
Note The default value (an asterisk, *) means that no signature checking is performed when testing whether a flow maps to this protocol element.

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

Figure 131: Select a Signature



Step 5 Select a signature from the list.

Note Select the Generic signature to allow a flow that has no matching signature in the protocol signature database to be mapped to this protocol element (if the flow also matches the IP protocol and port range of the protocol element).

Step 6 Click **OK**.

The Select a Signature dialog box closes.

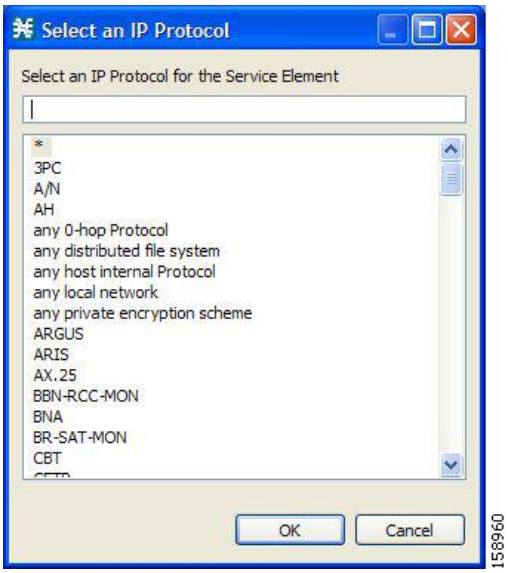
The selected signature is displayed in the Signature cell of the Protocol Settings dialog box.

Step 7 Click in the IP Protocol cell of the protocol element, and then click the Browse button that appears in the cell.

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

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

Figure 132: Select an IP Protocol



Step 8 Select an IP protocol from the list.

Step 9 Click **OK**.
The Select an IP Protocol dialog box closes

The selected IP protocol is displayed in the IP Protocol cell of the Protocol Settings dialog box.

Step 10 In the Port Range cell, enter a port or range of ports.
For a range of ports, use a hyphen between the first and last ports in the range.

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

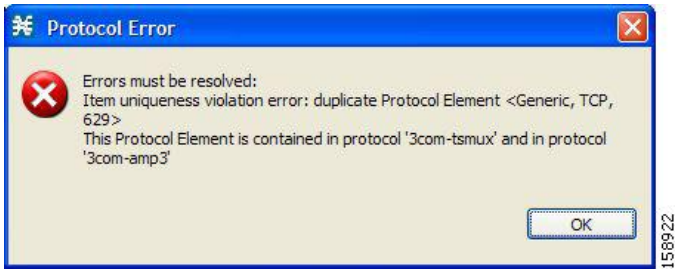
Only a flow whose port matches one of these ports are mapped to this protocol element.

The protocol element is defined.

Step 11 Click **Close**.
The Protocol Settings dialog box closes.

Instead, if the protocol element that you have defined is not unique in this service configuration, a Protocol Error message appears.

Figure 133: Protocol Error



Step 12 Click **OK**.

Step 13 Modify or delete the protocol element.

Step 14 Click **Close**.
The Protocol Settings dialog box closes.

Editing Protocol Elements

You can modify all protocol elements, even those protocol elements that are included in the Console installation.

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

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Protocols .
The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, select a protocol.

Step 3 In the Protocol Elements tab, select a protocol element.

Step 4 Click in the Signature cell of the protocol element, and then click the Browse button that appears in the cell.
The Select a Signature dialog box appears.

Step 5 Select a signature from the list.

Step 6 Click OK.
The Select a Signature dialog box closes.

Step 7 Click in the IP Protocol cell of the protocol element, and then click the Browse button that appears in the cell.
The Select an IP Protocol dialog box appears.

Step 8 Select an IP protocol from the list.

Step 9 Click OK.

The Select an IP Protocol dialog box closes.

Step 10 In the Port Range cell of the protocol element, enter a port or range of ports.
Changes to the protocol element are saved as you make them.

Step 11 Click Close.
The Protocol Settings dialog box closes.

Instead, if the protocol element that you have modified is not unique in this service configuration, a Protocol Error message appears.

Step 12 Click OK.

Step 13 Modify or delete the protocol element.

Step 14 Click Close.
The Protocol Settings dialog box closes.

Deleting Protocol Elements

You can delete all protocol elements, even those protocol elements that are included in the Console installation.

Procedure

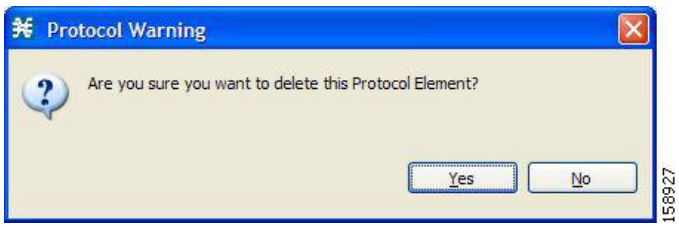
Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Protocols .
The Protocol Settings dialog box appears.

Step 2 Select a protocol in the Protocols tab.

Step 3 In the Protocol Elements tab, select a protocol element.

Step 4 In the Protocol Elements tab, click the Delete Protocol Element ( ) icon.
A Protocol Warning message appears.

Figure 134: Protocol Warning



Step 5 Click Yes.
The protocol element is deleted from the Protocol Elements tab.

Step 6 Click Close .
The Protocol Settings dialog box closes.

Introduction to Managing Zones

A zone is a collection of destination IP addresses; usually the addresses in one zone are related in some way.

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

BGP Autonomous System Dynamic Detection

The BGP Autonomous System (BGP AS) Dynamic Detection feature enables you to provision the BGP autonomous system as IP prefixes to the Cisco SCE zones.

With the BGP AS Dynamic Detection feature, you can:

- Add the complete AS number node and all the IP prefixes under it to a new zone.
- Add the IP Prefixes obtained from the AS number nodes to an existing zone.
- Add IP prefixes to a new zone.
- Delete IP prefixes from a zone.

For details, see the following sections:

- BGP AS Dynamic Detection Workflow, on page 196
- Enabling BGP As Dynamic Detection, on page 196
- Collecting and Storing the BGP Autonomous System Details, on page 197
- Creating a New Zone with Select BGP AS Numbers and Prefixes, on page 198
- BGP AS Numbers and Prefixes Color Schema, on page 199
- Updating a Zone with Select BGP AS Numbers and Prefixes, on page 200
- Deleting IP Prefixes from a Zone, on page 200

Viewing Zones

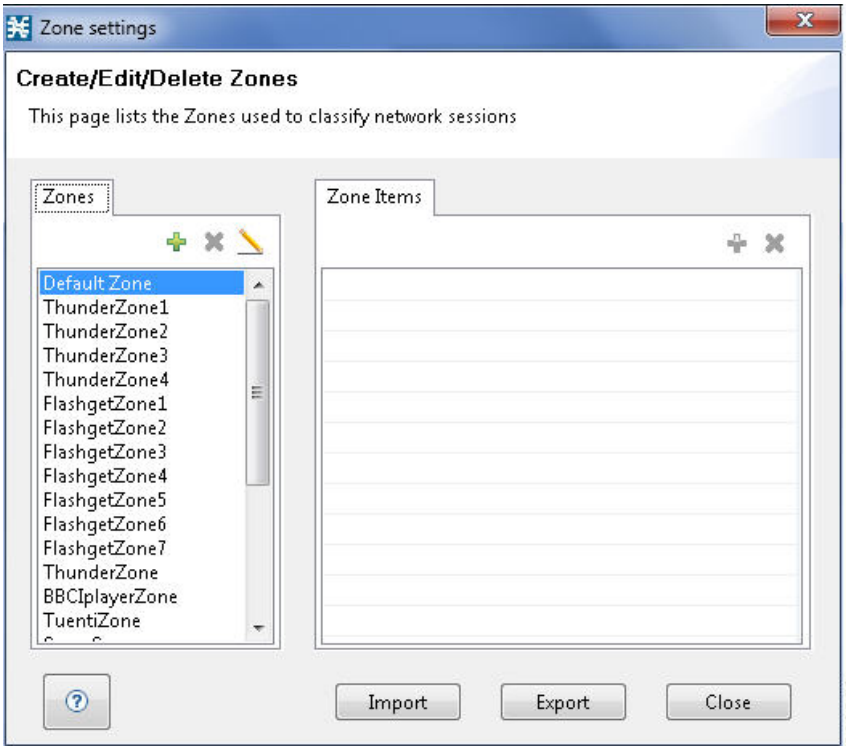
You can view a list of all zones and their associated zone items.

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > 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.

Figure 135: Zone Settings



Step 2 Click a zone in the list to display its zone items.
The zone items of the selected zone are displayed in the Zone Items tab.

Step 3 Click Close .

Timesaver If you enable the automatic zone provisioning, an Advanced Import button will be available. Click the Advanced Import button to import the BGP AS numbers and prefixes to create Zones. See the Creating a New Zone with Select BGP AS Numbers and Prefixes, on page 198 section.

Adding Zones

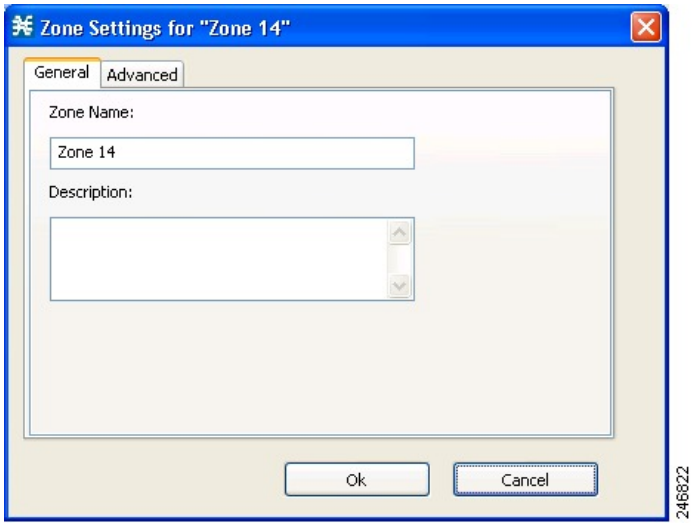
Procedure

Step 1 From the Classification tab in the left pane, choose **Configuration** > **Classification** > **Zones**.
The Zone Settings dialog box appears.

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

The Zone Settings dialog box appears.

Figure 136: Zone Settings

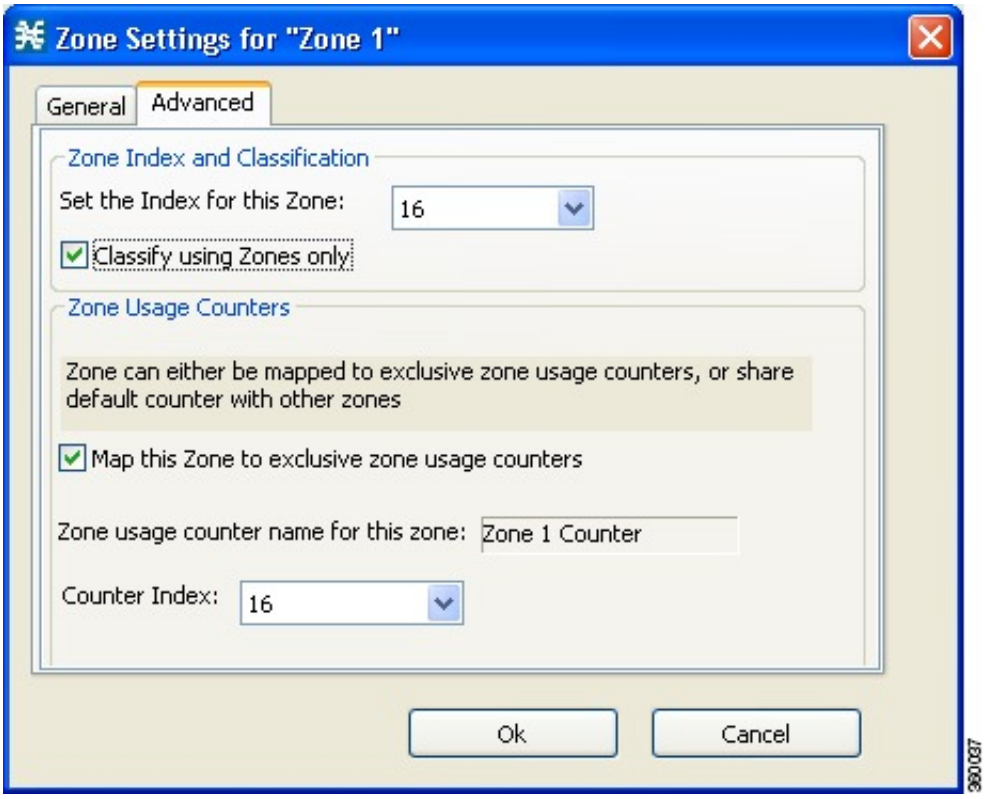


Step 3 In the Name field, enter a unique name for the new zone.

Step 4 From the Advanced tab, from the Zone Index drop-down list, select an ID for the zone. The zone ID must be a positive integer in the range from 1 to 32767.

Note The system provides the value of the zone ID. Do not modify this field.

Figure 137: Zone Settings - Advanced Tab



Step 5 (Optional) Check the Classify using zones only check box. Click Yes in the pop up window to confirm. If you enable this option, the Cisco SCE classifies the data flows based on the zone to which the data flows belong.

Note If you enable this option on an existing zone, every service element that references the selected zone is deleted.

Step 6 Check the Map this Zone to exclusive zone usage counters check box to map the Zone to exclusive zone usage counters, or share default counter with other zones.
The Zone Settings dialog box appears.

Step 7 From the Counter Index drop-down list, select an index for the zone.
The Counter Index must be a positive integer in the range from 1 to 1023.

Step 8 Click OK.
The Zone Settings dialog box closes.

What to Do Next

The new zone is added to the Zones tab. You can now add zone items. (See Adding Zone Items, on page 194 section.)

Editing Zones

You can modify zone parameters at any time.

To add, modify, or delete zone items, see Introduction to Managing Zone Items , on page 194 section.

Procedure

Step 1 From the Classification tab in the left pane, choose **Configuration** > **Classification** > **Zones**.
The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 Click the Edit Zone ( ) icon.
The Zone Settings dialog box appears.

Step 4 Modify fields in the dialog box.

a) In the Name field, enter a new name for the zone.

b) From the Zone Index drop-down list, select an ID for the zone.
The zone ID must be a positive integer in the range from 1 to 32767.

Note The system provides the value of the zone ID. Do not modify this field.

Step 5 Click **OK**.
The Zone Settings dialog box closes.

The new values of the zone parameters are saved.

Step 6 Click **Close**.
The Zone Settings dialog box closes.

Deleting Zones

You can delete any or all zones.

Procedure

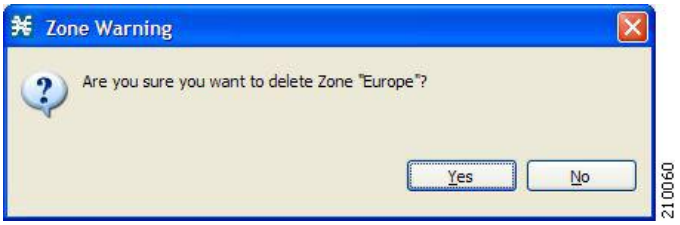
Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Zones .
The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

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

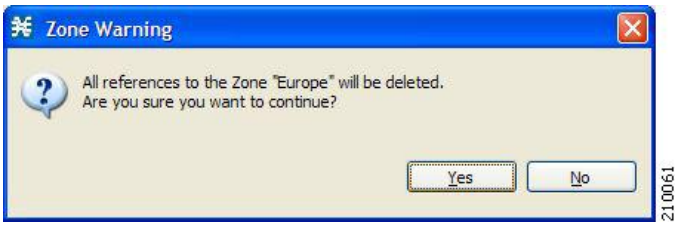
A Zone Warning message appears.

Figure 138: Zone Warning



Step 4 Click OK.
If any service element references the selected zone, a second Zone Warning message appears.

Figure 139: Zone Warning



Step 5 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 6 Click Close.
The Zone Settings dialog box closes.

Introduction to Managing Zone Items

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

Adding Zone Items

Procedure

Step 1 From the Classification tab in the left pane, choose **Configuration** > **Classification** > **Zones**.
The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 In the Zone Items tab, click the Add Zone Item ( ) icon.
A new line is added to the Zone Items table.

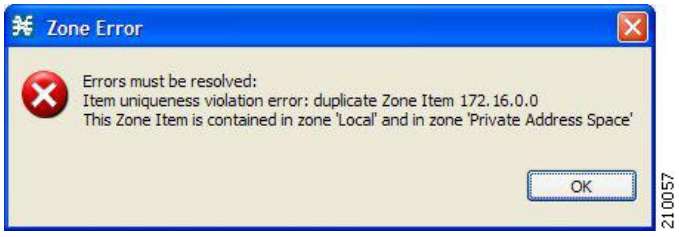
Step 4 Double-click the new list item and enter a valid value.
A valid value is either a single IP address (for example, 63.111.106.7 or ABCD:1111:97EF:F641:0F2A:ABCD:1111:97EF) or a range of IP addresses (for example, 194.90.12.0/24 or ABCD:1111:97EF:F641:0F2A:ABCD:1111:97EF/128). For IPv6 zones, the valid range is from 0 to 128.

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

Step 6 Click **Close**.
The Zone Settings dialog box closes.

Instead, if the zone item that you have defined is not unique in this service configuration, a Zone Error message appears.

Figure 140: Zone Error



Step 7 Click **OK**.

Step 8 Modify or delete the zone item.

Step 9 Click **Close**.
The Zone Settings dialog box closes.

Editing Zone Items

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Zones .
The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

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

Step 4 Enter a new value for the zone item.
A valid value is either a single IP address (for example, 63.111.106.7 or ABCD:1111:97EF:F641:0F2A:ABCD:1111:97EF) or a range of IP addresses (for example, 194.90.12.0/24 or ABCD:1111:97EF:F641:0F2A:ABCD:1111:97EF/128). For IPv6 zones, the valid range is from 0 to 128.

Step 5 Click Close.
The Zone Settings dialog box closes.

Instead, if the zone item that you have modified is not unique in this service configuration, a Zone Error message appears.

Step 6 Click OK.

Step 7 Modify or delete the zone item.

Step 8 Click Close.
The Zone Settings dialog box closes.

Deleting Zone Items

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Zones .
The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 In the Zone Items tab, select a zone item.

Step 4 In the Zone Items tab, click the Delete Zone Item () icon.
The zone item is deleted.

Step 5 Click Close .
The Zone Settings dialog box closes.

BGP AS Dynamic Detection Workflow

This section provides details on the BGP AS Dynamic Detection workflow:

1. When you run the asFetch.bat script, the script downloads the AS number and IP prefixes from the configured BGP router using the SNMP MIBs
2. The script converts the prefixes to IP ranges and stores the details in a local file. If you configure a scheduler to run the script periodically, during each run, the IP file gets overwritten with a new one.
3. Cisco SCA BB:
   a. Maps each zone name to the parameter of SCA BB zone configuration, such as Zone Index.
   b. Pushes parameters such as zone and zone items (BGP routes) to the Cisco SCE while applying the configuration.
   c. Configures the Services configured on various zones and pushes the configuration to the Cisco SCE.
4. Cisco SCE controls the service bandwidth based on the services configured on various zones.

Enabling BGP As Dynamic Detection

By default, BGP as Dynamic Detection is disabled on Cisco SCA BB.

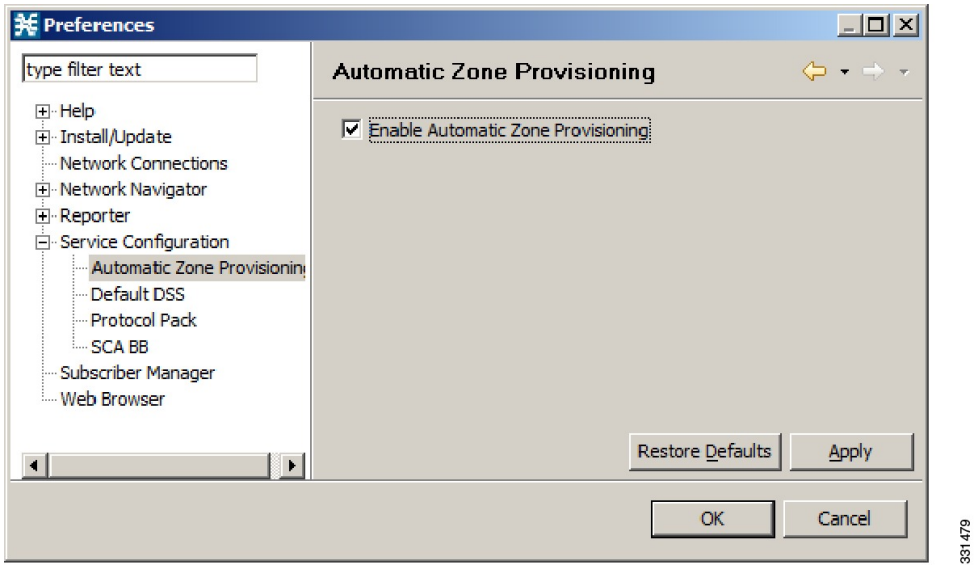
Procedure

Step 1 Choose **Windows** > **Preferences**.

Step 2 In the Preferences window, expand the Service Configuration.

Step 3 Click **Automatic Zone Provisioning**.

Step 4 Check the **Enable Automatic Zone Provisioning** check box.



Step 5 Click **Apply**.

Step 6 Click **OK**.

Collecting and Storing the BGP Autonomous System Details

The Cisco SCA BB asFetch script uses SNMP MIBs to fetch the BGP Autonomous System (BGP AS) numbers and prefixes.

The routerInfo.properties file, asFetch.bat, and asFetch.sh are in the sca_bb_util\bin folder.

Procedure

Step 1 Enter the router IP and SNMP community string in the routerInfo.properties file.
If AS numbers and IP prefixes have to be generated for more than one router IP, enter the router IP address of the community string separated by a comma (,) in the routerInfo.properties file.

Step 2 Run the asFetch.bat script.
You can run the script manually or use a scheduler to run the script periodically.

Run the asFetch.bat file to generate the BGPRouter<number>.csv files based on the number of IP addresses entered in the properties file. For example, if two IP addresses are specified in the properties file, The BGPRouter1.csv and BGPRouter2.csv files get generated.These .csv files contain the AS number and IP prefix details. These files can be imported from the Zone settings window.

The script fetches the AS number and IP prefix details and saves them in the BGPRouter<number>.csv file that is present in the same folder in which you have extracted the asFetch script.

Creating a New Zone with Select BGP AS Numbers and Prefixes

Before You Begin

Before attempting to add the BGP AS numbers and prefixes to zones, enable automatic zone provisioning and run the asFetch script to get the BGP AS details into the BGPRouter<number>.csv file.

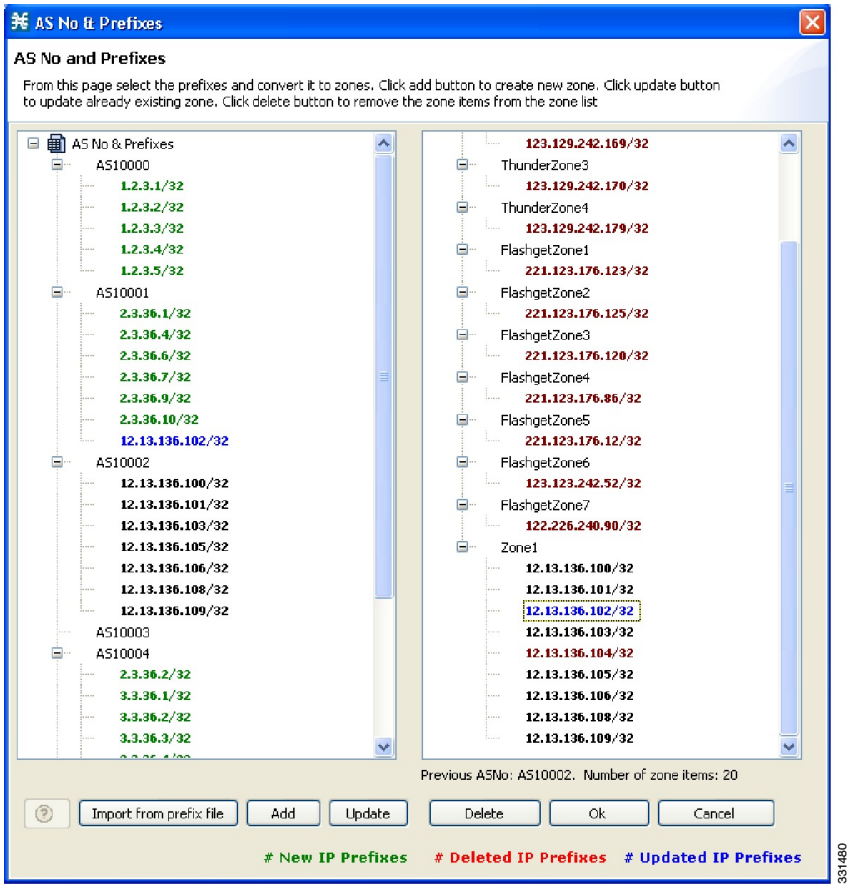
Procedure

Step 1 From the Service Configuration Editor window, choose **Configuration** > **Classification** > **Zones**.

Step 2 In the Zone Settings window, click **Advanced Import**.

Step 3 Browse to the folder in which the BGPRouter<number>.csv file is saved, and select the BGPRouter<number>.csv file.

Step 4 Click **Open**.
The AS No & Prefixes dialog box appears.



Step 5 Select the corresponding AS Number.

Step 6 Click **Add**.

Step 7 Enter a New Zone Name.

Step 8 Click **OK**.

Step 9 Click **OK**.

BGP AS Numbers and Prefixes Color Schema

The AS Number and Prefixes dialog box uses various colors to indicate new prefixes, prefixes added to a zone, or changes to the AS Number to which the prefix belongs.

Green color indicates a new prefix that does not belong to any zone. After you add the prefix to a zone, the color of the prefix in the prefix list and the zone changes to black. If you remove the prefix from the zone, the color of the prefix in the prefix list changes to green again.

Blue color indicates that the prefix has moved from one AS to another. This helps you decide whether to move the prefix to another zone.

Red color indicates that the prefix is not a part of the AS Numbers and Prefixes list.

Updating a Zone with Select BGP AS Numbers and Prefixes

Procedure

Step 1 From the Service Configuration Editor window, choose Configuration > Classification > Zones .

Step 2 In the Zone Settings window, click Advanced Import .

Step 3 Browse to the folder in which the BGPRouter<number>.csv file is saved and select the BGPRouter<number>.csv file.

Step 4 Click Open.
The AS No & Prefixes dialog box appears.

Step 5 Select the corresponding AS Number.

Step 6 Click Update.

Step 7 Choose a zone from the drop-down list.

Step 8 Click OK.

Step 9 Click OK.

Timesaver From the AS No & Prefixes dialog box, you can drag and drop the required AS numbers and IP prefixes to the required zones.

Deleting IP Prefixes from a Zone

You can delete IP prefixes only from a zone and not from the AS Numbers and Prefixes list.

Procedure

Step 1 Select the prefixes you want to delete.

Step 2 Click Delete .

Introduction to Managing Protocol Signatures

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

Viewing Protocol Signatures

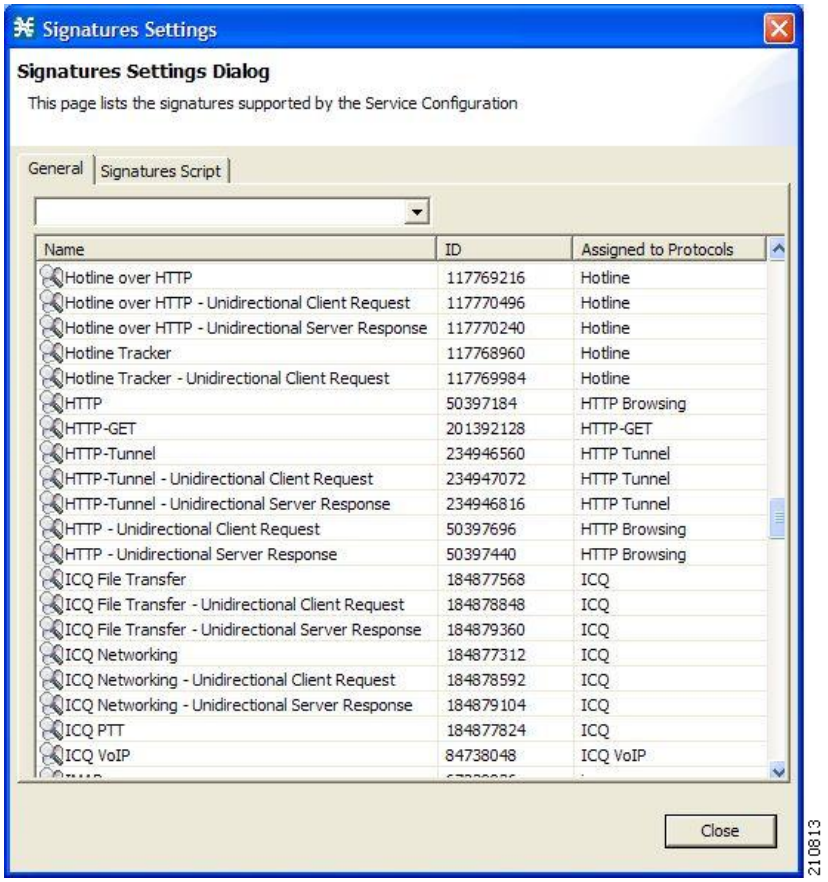
You can view a list of all signatures and the protocol to which each is assigned.

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Signatures Settings .

The Signatures Settings dialog box appears.

Figure 141: Signatures Settings



Step 2 Click Close.
The Signatures Settings dialog box closes.

Filtering the Protocol Signatures List

You can filter the signature by type, so that the Signatures Settings dialog box lists only the selected type of signature.

The signature categories are:

- DSS Contributed Signatures
- Not Assigned to any Protocol
- P2P Signatures
- VoIP Signatures

- SIP Signatures
- Worm Signatures
- Packet Stream Pattern Based Protocols Signatures
- Unidirectionally Detected Signatures
- Behavioral Signatures
- E-Mail and Newsgroups Signatures
- Gaming Signatures
- HTTP Signatures
- Instant Messaging Signatures
- Net Admin Signatures
- Video Signatures
- Tunneling Signatures
- ClickStream Signatures



Note Some signatures belong to more than one category.

Procedure

Step 1 From the Console main menu, choose Configuration > Classification > Signatures Settings .
The Signatures Settings dialog box appears.

Step 2 From the drop-down list, select the type of signature to display.
The signatures of the selected type appear in the dialog box.

Step 3 Click Close.
The Signatures Settings dialog box closes.

Dynamic Signatures

New protocols are being introduced all the time. Dynamic signatures is a mechanism that allows new protocols to be added to the protocol list and, from there, to service configurations. Dynamic Signature is especially useful for classifying the traffic of a new protocol (for example, a new P2P protocol in a P2P-Control solution).

- Installing new signatures to an active service configuration is described in Working with Protocol Packs , on page 55.
- Creating and modifying signatures is described in The Signature Editor Overview, on page 491.
- Using **servconf** , the Cisco SCA BB Server Configuration Utility, to apply signatures is described in The Cisco SCA BB Service Configuration Utility , on page 509.

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

Dynamic Signature Script Files

Dynamic signatures are provided in special Dynamic Signatures Script (DSS) files that you can add to a service configuration using either the Console or the Service Configuration API. After a DSS file is imported into a service configuration, the new protocols it describes:

- Appear in the protocol list.
- May be added to services.
- Are used when viewing reports.

To simplify the configuration of new protocols added by a DSS, the DSS may specify a Buddy Protocol for a new protocol. If, when loading a DSS, the application encounters the Buddy Protocol, it automatically duplicates the set of service elements that use the Buddy Protocol, and replaces all references to the Buddy Protocol with references to the new protocol. The association of the new protocol to services matches that of the Buddy Protocol.

The following configuration actions are performed automatically when you import a DSS into a service configuration:

- Signatures are updated and new signatures are loaded.
- Protocol elements are created for new signatures of existing protocols.
- New protocols are added to the protocol list, and protocol elements are created for them.
- Service elements are created for new protocols according to the configuration of Buddy Protocols.

The import procedure preserves all service and protocol settings.



Note After importing a DSS, associate the newly added protocols with services.

Cisco or its partners releases DSS files periodically in accordance with customer requirements and market needs.

DSS files contain new protocols and signatures, and update previously defined signatures. Updating a service configuration with the new DSS is explained in Importing a Dynamic Signature Script into a Service Configuration , on page 205.



Note You can create your own DSS files or modify the Cisco release DSS file using the Signature Editor tool (see Managing DSS Files Overview, on page 491 section).

Viewing Information About the Current Dynamic Signatures

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Signatures Settings .

The Signatures Settings dialog box appears.

Step 2 Click the Signatures Script tab.
The Signatures Script tab opens.

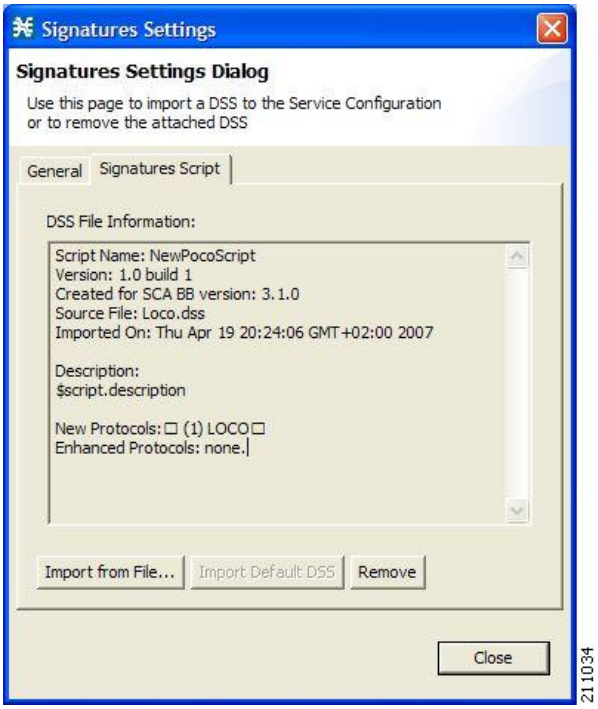
- If no DSS file was imported into the current service configuration, the Signatures Settings dialog box displays a message informing you of this.

Figure 142: Signature Settings



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

Figure 143: Signature Settings



Step 3 Click Close.
The Signatures Settings dialog box closes.

Importing a Dynamic Signature Script into a Service Configuration

You can import signatures into a service configuration from a DSS file provided by Cisco or one of its partners (described in this section), or from a DSS file that you have created or modified using the Signature Editor tool (see Managing DSS Files Overview, on page 491 section).

Note It is recommended that you import the latest default DSS file (see Importing the Default DSS File Automatically , on page 211 section) when creating a service configuration, and that you use this option only to apply a new DSS to existing service configuration.

Procedure

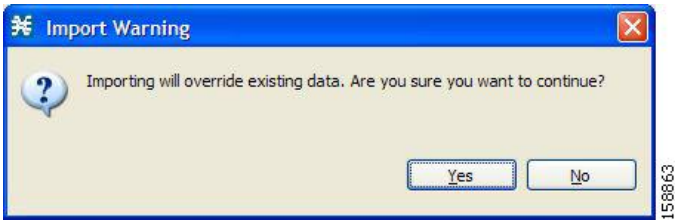
Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Signatures Settings.

The Signatures Settings dialog box appears.

Step 2 Click the Signatures Script tab.
The Signatures Script tab opens.

Step 3 Click Import from File.
An Import Warning message appears.

Figure 144: Import Warning



Step 4 Click Yes.
The Import from file dialog box appears.

Step 5 Browse to the DSS file and click Open .
The Import from file dialog box closes.

The signatures in the DSS file are imported into the service configuration.

Information about the imported signatures and their DSS file is displayed in the Signatures Settings dialog box.

Step 6 Click Close.
The Signatures Settings dialog box closes.

Removing Dynamic Protocol Signatures

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

Note The DSS file is not deleted.

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Signatures Settings .
The Signatures Settings dialog box appears.

Step 2 Click the Signatures Script tab.
The Signatures Script tab opens.

Step 3 Click Remove .

A Dynamic Signature Script Confirmation message appears.

Figure 145: Dynamic Signature Script Confirmation



Step 4 Click OK.
If any service element references a protocol whose signature is included in the imported DSS file, a Dynamic Signature Script Removal Error message appears.

Figure 146: Dynamic Signature Script Removal Error



Step 5 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 6 Click Close.
The Signatures Settings dialog box closes.

The Default DSS File

Whenever a protocol pack becomes available from Cisco (or one of its partners), you should update offline service configurations (stored as PQB files on the workstation). The protocol pack (see Protocol Packs , on page 55 section) is provided as either an SPQI file or a DSS file.

You can either offer updates automatically to every service configuration created or edited at the workstation, or apply them from the workstation to the Cisco SCE platform. You make the latest update available by installing the most recent DSS or SPQI file as the default DSS file. You can install the file on the workstation either from the Console or by using The Cisco SCA BB Signature Configuration Utility , on page 513.

- The default DSS file is automatically offered for import when you perform any service configuration operation (such as creating a new service configuration or editing an existing one) from the Console on a service configuration that was not yet updated.
- The default DSS file is imported by default when any service configuration operation (such as applying an existing service configuration) is performed using **servconf**, The Cisco SCA BB Signature Configuration Utility , on page 513. 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.

Introduction to Setting and Clearing the Default DSS File

The default DSS file should normally be the latest protocol pack provided by Cisco (or one of its partners). If necessary, modify the protocol pack using the Signature Editor tool (see Editing DSS Files , on page 504 section) to add signatures of new protocols until they become available from Cisco.

Whenever a new protocol pack becomes available, set it as the default DSS file. There is no need to clear the current default DSS file; it is overwritten by the new protocol pack.

Setting a Protocol Pack as the Default DSS File

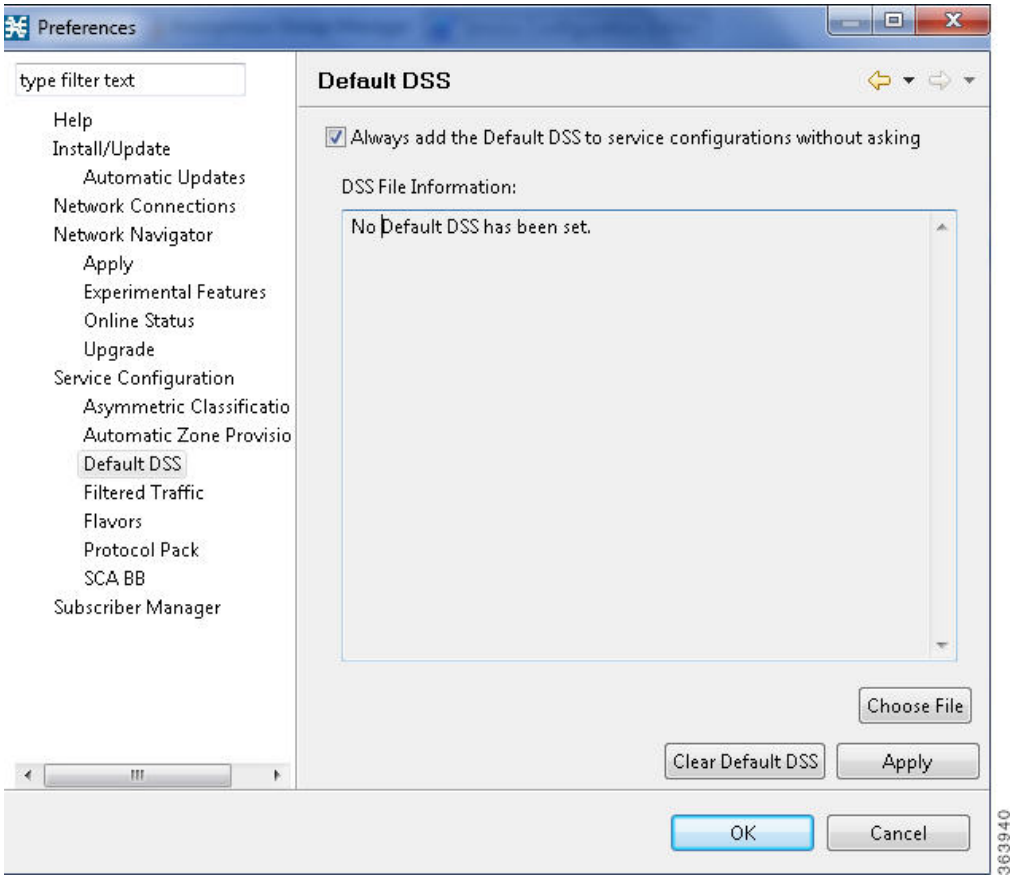
Procedure

Step 1 From the Console main menu, choose Window > Preferences .
The Preferences dialog box appears.

Step 2 From the menu tree in the left pane of the dialog box, choose Service Configuration > Default DSS .

The Default DSS area opens in the right pane of the dialog box.

Figure 147: Preferences



Step 3 Click Choose File.
An Open dialog box appears.

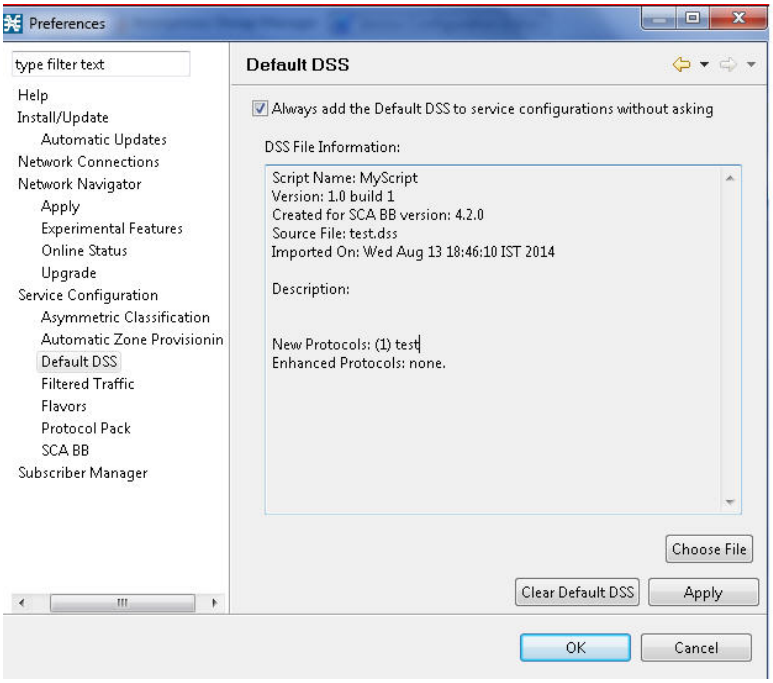
Step 4 From the Files of type drop-down list, select the file type of the protocol pack.

Step 5 Browse to the protocol pack.

Step 6 Click Open.
The Open dialog box closes.

Information about the default DSS file is displayed in the Default DSS area of the Preferences dialog box.

Figure 148: Preferences - Default DSS



Step 7 Click OK.
The DSS file is copied to C:\Documents and Settings\<username>\.p-cube\default3.6.5.dss as the default DSS file. In Windows 7, the DSS file is copied to C:\Users\<username>\.p-cube\.

The Preferences dialog box closes.

Clearing the Default DSS File

Procedure

Step 1 From the Console main menu, choose **Window** > **Preferences** .
The Preferences dialog box appears.

Step 2 From the menu tree in the left pane of the dialog box, choose **Service Configuration** > **Default DSS**.
The Default DSS area opens in the right pane of the dialog box.

Step 3 Click **Clear Default DSS**.
The default DSS file, C:\Documents and Settings\<username>\.p-cube\default4.1.0.dss, is deleted. In Windows 7, the default DSS file is C:\Users\<username>\.p-cube\default4.1.0.dss.

All information is deleted from the Default DSS area.

Note Deleting the default DSS file does not remove the imported dynamic signatures from the current service configuration.

Step 4 Click **OK**.
The Preferences dialog box closes.

Introduction to Importing Dynamic Signatures from the Default DSS File

If a default DSS file is installed, the application offers to import the dynamic signatures from the file when you create a new service configuration or when you open an existing service configuration that has not imported the signatures. Alternatively, you can manually import the dynamic signatures.

Importing the Default DSS File Automatically

Procedure

Step 1 Open an existing service configuration or create a new one.
A Default Signature message appears.

Figure 149: Default Signature



Step 2 Click **Yes** to import the default DSS file; click **No** to continue without importing the default DSS file.

Importing the Default DSS File Manually

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Signatures Settings .
The Signatures Settings dialog box appears.

Step 2 Click the Signatures Script tab.

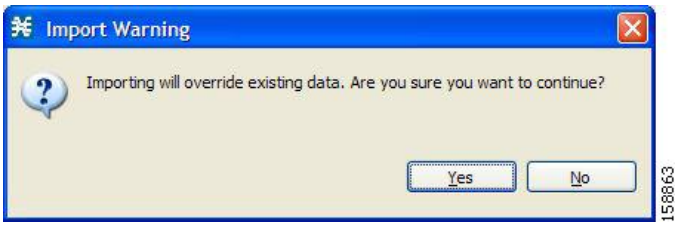
The Signatures Script tab opens, with the Import Default DSS button enabled.

Figure 150: Signatures Settings



Step 3 Click Import Default DSS.
An Import Warning message appears.

Figure 151: Import Warning



Step 4 Click Yes .
The signatures in the default DSS file are imported into the service configuration.

The Import Default DSS button is dimmed.

Information about the imported signatures and the default DSS file is displayed in the Signatures Settings dialog box.

Step 5 Click Close.
The Signatures Settings dialog box closes.

Introduction to Managing Flavors

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

Flavors are based on specific Layer 7 properties. For example, users can associate an HTTP flow with a service based on different parts of the destination URL of the flow.

Note When you configure flavors, you cannot configure < and > symbols to be part of a URL.

Flavors are supported only for small number of protocols, and for each such protocol there are different applicable flavor types. Flavor types are listed in the table in the following section.

There is a maximum number of flavor items for each flavor type (see Maximum Number of Flavor Items per Flavor Type , on page 224 section). For each flavor type, every flavor item must be unique.

Note If unidirectional classification is enabled in the active service configuration, flavors are not used for traffic classification.

Flavor Types and Parameters

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

When Layer 7 application properties are used as session parameters, such as with an HTTP User Agent, They are treated as character strings.

Layer 7 parameter-based flavor items may apply to the Layer 7 prefix (parameter beginning), Layer 7 suffix (parameter end), or a combination of Layer 7 prefixes and suffixes. A partial string must be followed by “*” in a prefix and preceded by “*” in a suffix.

Table 6: Cisco SCABB Flavors

Flavor Type	Matched Session Parameters	Valid Values
HTTP Composite	HTTP User Agent, HTTP URL, HTTP Cookie and HTTP Referer flavors serve as session parameters.	<HTTP User Agent flavor, HTTP URL flavor, HTTP Cookie flavor, HTTP Referer flavor> • The flavors can be chosen using flavor browsing.

Flavor Type	Matched Session Parameters	Valid Values
HTTP User Agent	HTTP User-Agent retrieved from the HTTP <User-Agent prefix> Request header field, from the beginning of the Request header until the first "/". For example, if the HTTP Request header field is Mozilla/4.0, the HTTP User Agent retrieved is Mozilla. If you want to configure the HTTP User Agent flavor with a Forward slash (/), set the value of the GT_CLS_ENABLE_FULL_USER_AGENT_BASED_FLAVOR_CALCULATION tunable to True.	<User-Agent prefix> Examples: • <Moz*> matches all HTTP sessions with User-Agent field starting with "Moz". • <Mozilla> matches all HTTP sessions with User-Agent field equal to "Mozilla". • The maximum key length is 32 characters.
HTTP URL	• Host—Retrieved either from the HTTP Host header field or from the Request URL. In the latter case, the section from the beginning of the URL until the first "/" is considered the Host. • Path—Retrieved from the HTTP URL, the section from the first "/" to the "?". • URL parameters—Any string following the "?" (You do not need to start the params with "?").	

Flavor Type	Matched Session Parameters	Valid Values
HTTP Cookie	Cookie “Key-Value” pairs that are retrieved from the HTTP Request header Cookie field. A Cookie may consist of many “Key-Value” pairs; however, only the first three pairs are calculated. The Cookie flavor calculation stops when one of the “Key-Value” pairs matches the specification, or when it has exceeded the three pair limit.	<key prefix, value prefix> • For example: <act*,*> matches any Cookie pair where the Key begins with “act”, regardless of the Value. • A flavor can be configured so that the Value field is required to be empty. In this case, this field should be left empty in the flavor item. • White spaces are not allowed, “=” is not allowed, and “*” is only allowed at the end of the Key or Value. • The maximum key length is 100 characters for both the Key and Value fields
HTTP Referer	Similar to HTTP URL, but the parameters are retrieved from the Referer HTTP header field.	
HTTP Content Category	Content Categories can be imported using the Import dialog box or the HTTP Content Filtering Settings dialog box.	Value selected from Select a Content Category dialog box.
RTSP User Agent	RTSP User-Agent field that is retrieved from the RTSP message header.	<RTSP User Agent prefix> • For example: <abc*> matches all RTSP sessions where the User-Agent starts with “abc”. • The maximum key length is 128 characters
RTSP Host Name	RTSP Host field that is retrieved from the RTSP message header.	<RTSP Host suffix> • For example: <*abc> matches all RTSP sessions where the Host ends with “abc”. • The maximum key length is 128 characters

Flavor Type	Matched Session Parameters	Valid Values
RTSP Composite	RTSP User Agent and RTSP Host Name flavors serve as session parameters.	<RTSP User Agent flavor, RTSP Host Name flavor>
SIP Source Domain	SIP Source Host field that is retrieved from the SIP message header.	<SIP Host suffix> • For example: <*abc> • The maximum key length is 128 characters
SIP Composite	SIP Source Host and SIP Destination Host serve as session parameters.	<SIP source domain, SIP destination domain>
SIP Destination Domain	SIP Destination Host field that is retrieved from the SIP message header.	<SIP Host suffix> • For example: <*abc> • The maximum key length is 128 characters
SMTP Host Name	SMTP Host field that is retrieved from the SMTP message header	• <SMTP Host suffix> • For example: <*abc> • The maximum key length is 128 characters
ToS	DSCP value extracted from the IP header	DSCP ToS (integer from 0 through 63)

Note Composite Flavors are pairs of two defined flavors.

Viewing Flavors

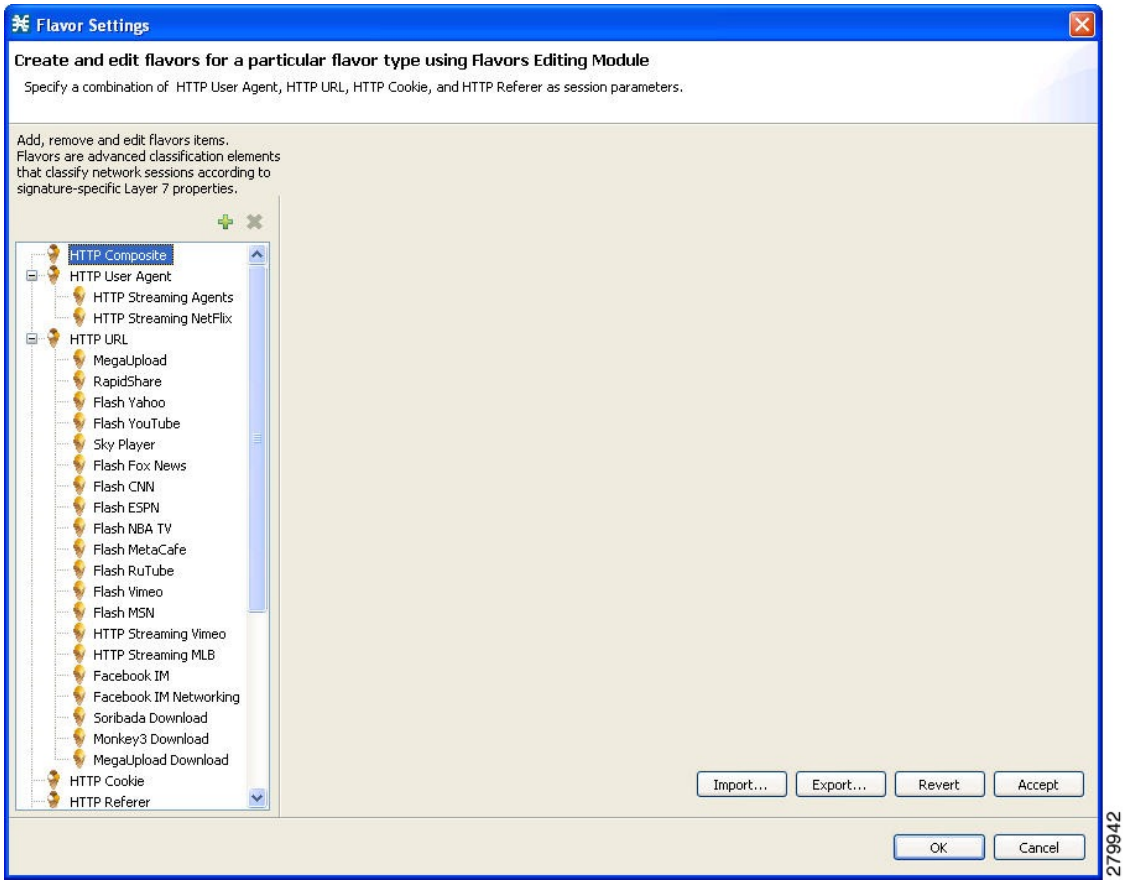
You can view a list of all flavors and their associated flavor items.

Procedure

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Flavors**.

The dialog box appears.

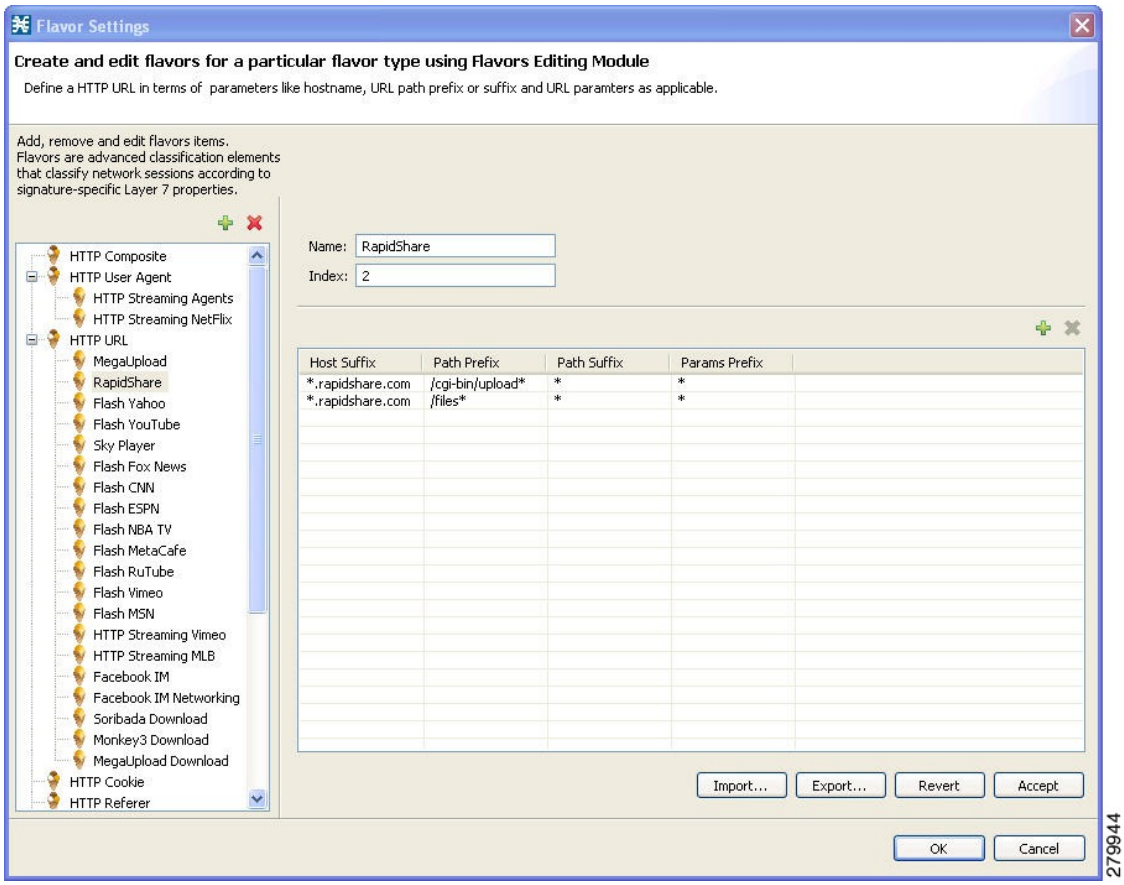
Figure 152: Flavor Settings



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

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

Figure 153: Flavor Settings



The flavor items are displayed in the right area.

Step 3 Click **OK**.
The Flavor Settings dialog box closes.

Adding Flavors

You can import flavors from a CSV file. CSV files can be created by exporting flavors or created manually as described in the “CSV File Formats” chapter of Cisco Service Control Application Suite for Broadband Reference Guide .

You can add any number of flavors to a service configuration.

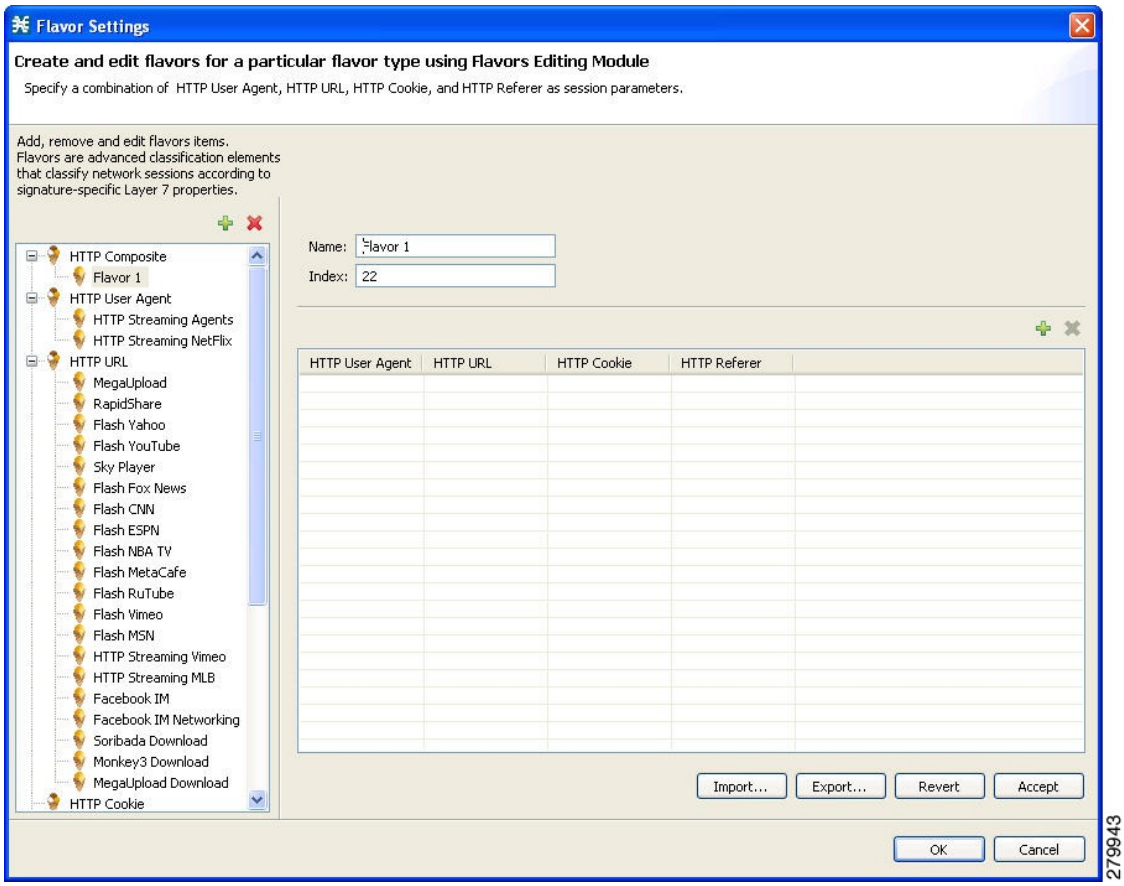
Procedure

Step 1 From the Classification tab in the left pane, choose **Configuration > Classification > Flavors**.
The Flavor Settings dialog box appears.

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

Step 3 Click the Add Flavor ( ) icon.
A new flavor of the selected type is added to the flavor tree.

Figure 154: Flavor Settings - Adding Flavors



Step 4 In the Name field, enter a name for the new flavor.
Note You can use the default name for the flavor. It is recommended that you enter a meaningful name.

Step 5 (Optional) In the Index field, enter a unique integer value.
Note Cisco SCA BB provides a value for the Index. There is no need to change it.
The flavor index must be a positive integer in the range from 1 to 2147483647.

You have defined the flavor. You can now add flavor items. (See Adding Flavor Items, on page 224 section.)

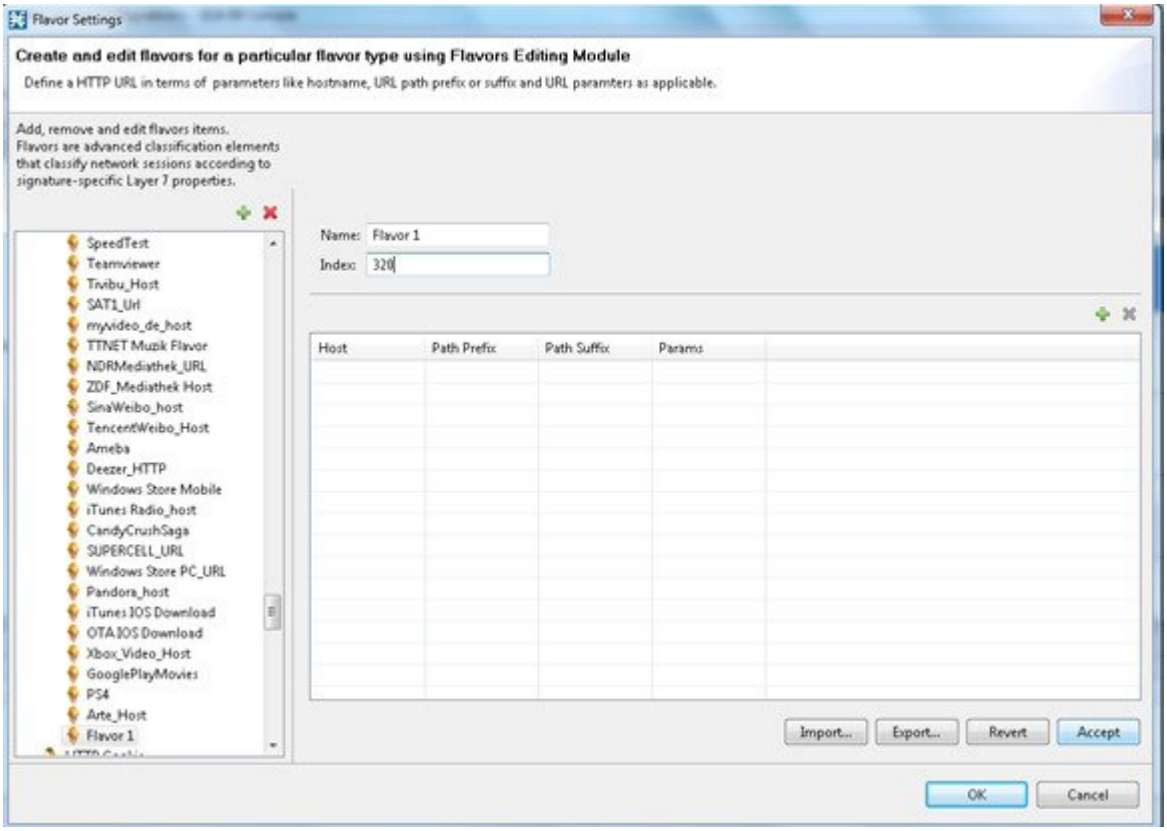
Adding 2M URL support

The SCABB supports up to 2 million (2M) HTTP URLs in the SCE 10k platform and supports up to 500k URLs in the SCE 8k platform. The URLs are available in the look-up table (LUT). The 2M URL is applied for SCE 10k through servicing API option and for SCE 8k through SCAB console.

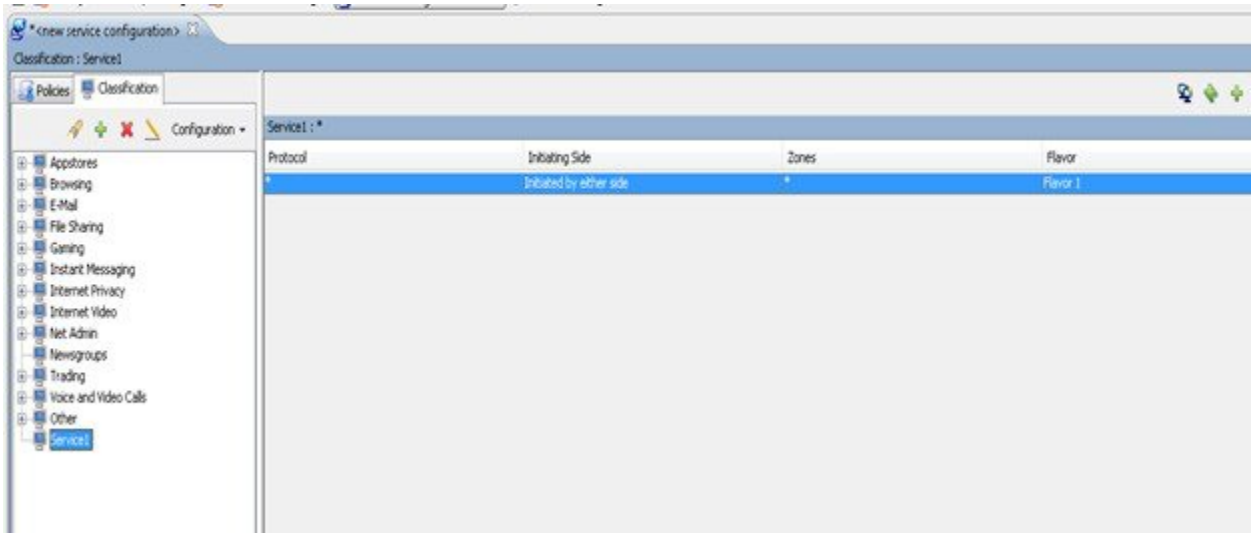
To add 2M URL support,

Procedure

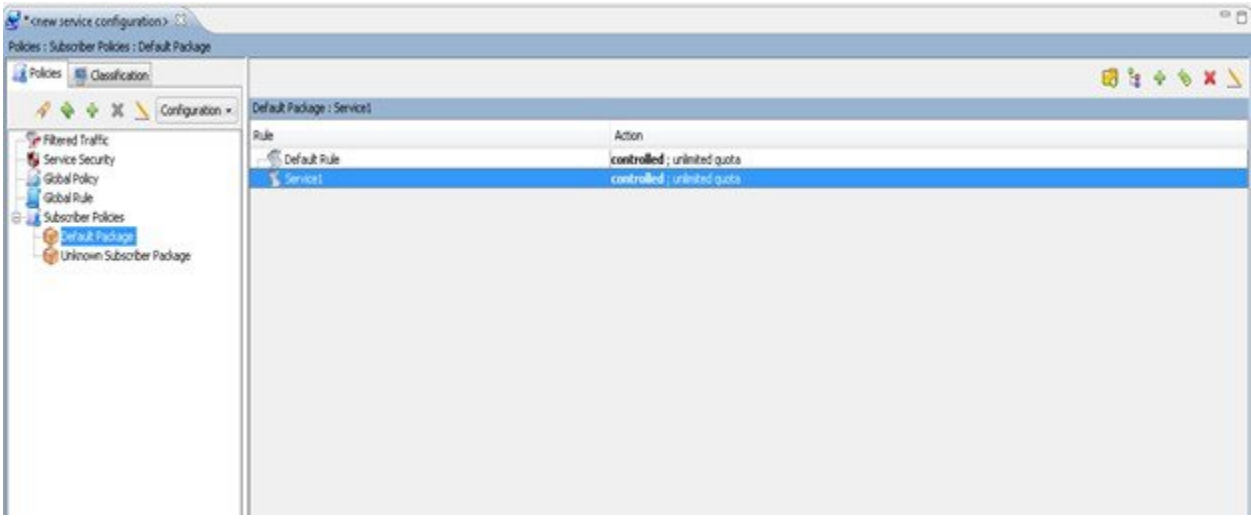
Step 1 Create an empty flavor with a respective CSV file by providing a flavor name and a flavor ID in the Flavors setting dialog box. For example: Flavor 1(Name), 51(ID).



Step 2 Create a new service with the newly created flavors.



Step 3 Create a rule with the newly added service under the package.



Step 4 Apply the policy with the above settings from SCABB console.

Step 5 Navigate to SCABB built management folder, and extract the bin folder and the lib folder from the sca_bb_util.tgz zip folder available in the SCABB built management folder.

Step 6 Open the command window and provide a CSV file path similar to the path provided for CLI commands for PQB.

Step 7 Edit the servconf.bat file in the bin folder to increase the default JVM memory by setting the VM Arguments as VMARGS="-Xbootclasspath/p:%SCAS_BB_HOME%/lib/opendmk.jar" -Xms40m -Xmx1024m -Duser.country=US -Duser.language=en -Xms512m - Xmx1280m.

Step 8 Enter the following command in the command window to import the 2M flavors in the CSV to SCE, where the previous policy is applied:
servconf.bat --se "SCE IP" --username admin --password cisco --apply --file "CSV file path".

Note It will take more than an hour for the policy to get updated and hence the user needs to wait until the CLI gets disconnected from the SCE.

Restrictions:

- Easy format CSV files are not supported.
- Multiple CSV files are not supported. So the user is recommended to maintain a single 2M URL CSV file.
- The CSV file corresponding to the policy that has been applied via API is not stored on the Service Control Engine (SCE). So, the user can view the policy applied only through SCABB.
- The user is recommended to apply policy through SCABB first and then through API, if it is done in reverse order all the 2M URLs in LUT will be overwritten. To retrieve the overwritten 2M URLs, the CLI has to be re-executed.

Caution The above configuration can be done only after increasing the size of HTTP URL flavor LUT to 2M.

Editing Flavors

You can modify flavor parameters at any time.

To add, modify, or delete flavor items, see Introduction to Managing Flavor Items, on page 223 section .

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Flavors .
The Flavor Settings dialog box appears.

Step 2 In the flavor tree, select a flavor.
The name and index of the flavor (and its flavor items) are displayed in the right area.

Step 3 Modify fields in the dialog box:

a) In the Name field, enter a new name for the flavor.

b) In the Index field, enter a new, unique index for the flavor.
The flavor index must be a positive integer in the range from 1 to 2147483647.

Step 4 Click OK.
The Flavor Settings dialog box closes.

Deleting Flavors

You can delete any or all flavors.

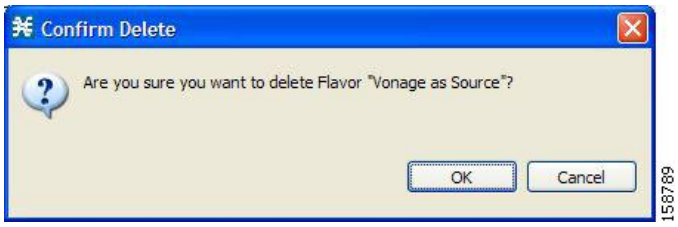
Procedure

Step 1 From the Classification tab in the left pane, choose **Configuration** > **Classification** > **Flavors** .
The **Flavor Settings** dialog box appears.

Step 2 In the flavor tree, right-click a flavor.
A popup menu appears.

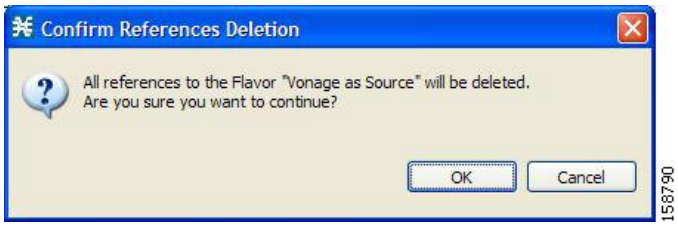
Step 3 Click the Delete ( ) icon.
A Confirm Delete message appears.

Figure 155: Confirm Delete



Step 4 Click OK.
If any service element references the selected flavor, a Confirm References Delete message appears.

Figure 156: Confirm References Deletion



Step 5 Click Yes.
Every service element that references the selected flavor is deleted.

The flavor is deleted and is no longer displayed in the flavor tree.

Step 6 Click Close.
The Flavor Settings dialog box closes.

Introduction to Managing Flavor Items

A flavor is a collection of related flavor items.

A flavor item is a value of a property or properties of a flow. These properties depend on the flavor type (see Flavor Types and Parameters , on page 213 section).

There is a maximum number of flavor items for each flavor type. For each flavor type, every flavor item must be unique.

Maximum Number of Flavor Items per Flavor Type

Table 7: Maximum Number of Flavor Items per Flavor Type

Flavor Type	Maximum No. of Flavor Items
HTTP Composite	10,000
HTTP User Agent	128
HTTP URL	100,000
HTTP Cookie	100
HTTP Referer	100
HTTP Content Category	—
HTTPS Client Hello	200,000
HTTPS Certificate	200,000
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
ToS	64

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).

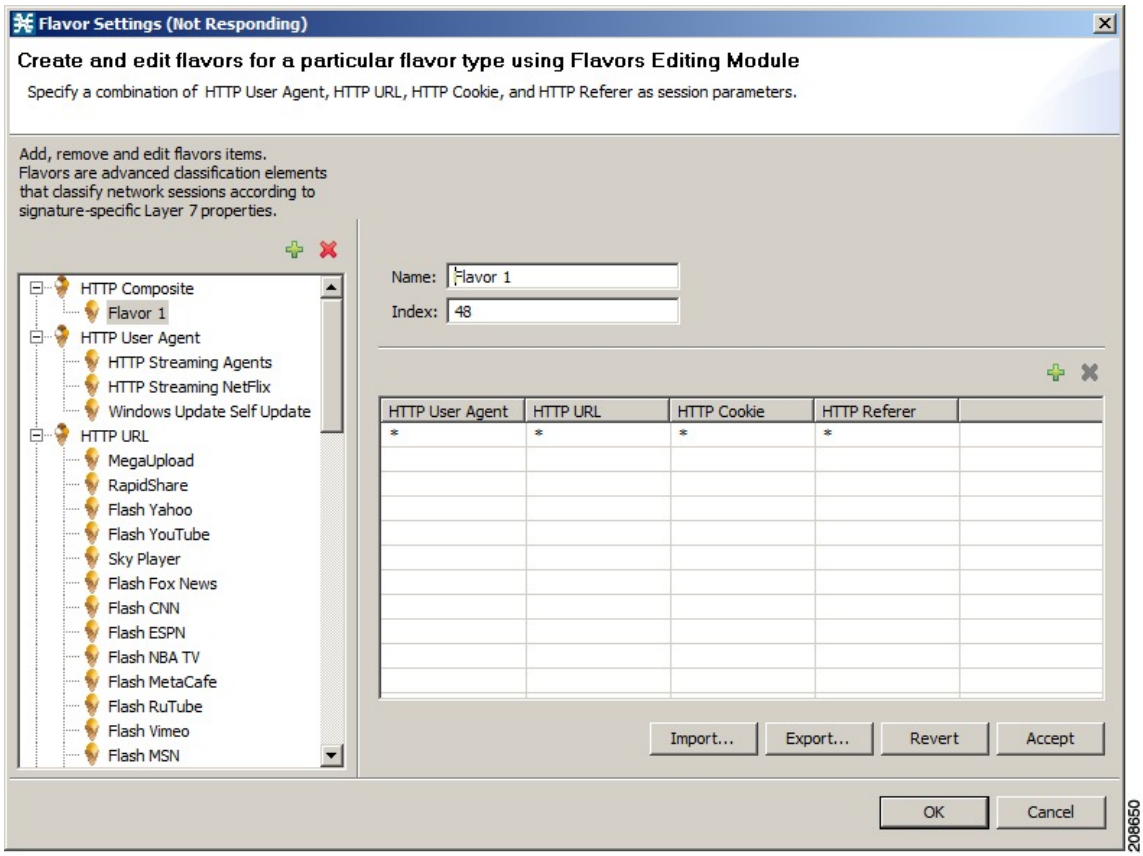
Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Flavors .
The Flavor Settings dialog box appears.

Step 2 In the flavor tree, click a flavor.

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

Figure 157: Flavor Settings



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 213 section).

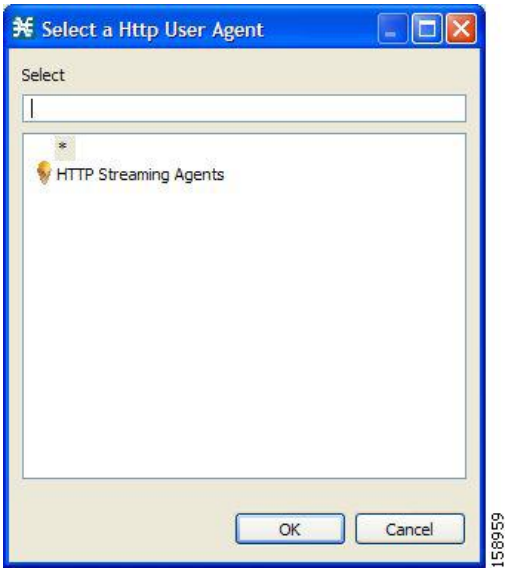
The new flavor item has a default value of all wild cards (*, asterisks).

Step 4 For each cell of the new flavor item, click the asterisk and then enter an appropriate value.
For composite flavors and for the HTTP Content Category flavor:

a) Click the asterisk.
A Browse button is displayed in the cell.
b) Click the Browse button.

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

Figure 158: Select an HTTP User Agent



c) Select an appropriate value from the list.
d) Click OK.
The Select dialog box closes.

The selected value is displayed in the cell.

Step 5 Repeat Steps 3 and 4 for other flavor items.

Step 6 Click OK.
The Flavor Settings dialog box closes.

Editing Flavor Items

Procedure

Step 1 From the Classification tab in the left pane, choose **Configuration** > **Classification** > **Flavors** .
The Flavor Settings dialog box appears.

Step 2 In the flavor tree, select a flavor.

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

Step 4 For each cell of the selected flavor item, click the asterisk and then enter an appropriate value.
For composite flavors and for the HTTP Content Category flavor:

a) Click the asterisk.
A Browse button is displayed in the cell.

b) Click the **Browse** button.
A Select dialog box appears, displaying all valid values for the parameter.

c) Select an appropriate value from the list.

d) Click **OK**.
The Select dialog box closes.

The selected value is displayed in the cell.

Step 5 Click **OK**.
The Flavor Settings dialog box closes.

Deleting Flavor Items

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Flavors .
The Flavor Settings dialog box appears.

Step 2 In the flavor tree, select a flavor.

Step 3 In the flavor item list, right-click anywhere in a flavor item.
A popup menu appears.

Step 4 Click the Delete () icon.
The flavor item is deleted and is no longer displayed in the flavor item list.

Step 5 Click Close .
The Flavor Settings dialog box closes.

Example on How to Import a List of URLs and Block Them

The following example shows how to import a URL file and configure the Cisco SCE to block these URLs

Procedure

Step 1 Create a new flavor under the HTTP URL flavor type.
For details, see the Adding Flavors, on page 218 section.

Step 2 Import a CSV file containing the URLS you wish to block.
For further information, see Importing Service Configuration Data , on page 150 section.

Note The CSV file formats are described in the “CSV File Formats” chapter of Cisco Service Control Application Suit for Broadband Reference Guide .

Step 3 Define a Service.

For further information, see Adding a Service to a Service Configuration , on page 160 section.

Step 4 Within the defined Service, add a service element that uses the new Flavor.
For further information, see Adding Service Elements , on page 168 section.

Step 5 Add a rule to the package in which you want to block the URLs, and associate it with the new Service.
For further information, see Adding Rules to a Package , on page 333 section.

Step 6 Configure the rule to block the flow.
For further information, see Defining Per-Flow Actions for a Rule , on page 335 section.

Introduction to Managing Content Filtering

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

Cisco SCA BB provides content filtering by integrating with a SurfControl Content Portal Authority (CPA) server.

Note Content filtering is not supported when unidirectional classification is enabled.

Information About Content Filtering

The Cisco HTTP Content Filtering solution consists of:

- The Cisco SCE application
- The Cisco CPA client
- The SurfControl CPA server

The Cisco SCE application classifies each HTTP flow according to the category returned by the CPA server. This classification is then used for Cisco SCA BB traffic control and reporting. For example, you can define a rule to block browsing of the “Adult/Sexually Explicit” category or to generate reports on the volume consumed by browsing the “Kids” or “Shopping” categories.

The Cisco SCE Application

The Cisco service control application runs on the Cisco SCE platform. It forwards HTTP URLs that it extracts from traffic to the CPA client and uses the categorization results to classify the original HTTP flow to a service. This classification is then used for normal Cisco SCA BB traffic control and reporting.

The Cisco SCE application communicates with the CPA client using Raw Data Records (RDRs). See Configuring the RDR Formatter , on page 230 section.

The Cisco CPA Client

The Cisco CPA client runs on the Cisco SCE platform. It sends URL queries to the CPA server for categorization, and updates Cisco SCA BB with the categorization results.

The CPA client is installed as part of the Cisco SCA BB application (PQI) installation. Use the Cisco SCE platform Command-Line Interface (CLI) (see The Content Filtering CLI, on page 229 section) to configure and monitor the client.

The SurfControl CPA Server

The CPA server runs on a dedicated machine. It receives categorization requests from the CPA client, connects to the SurfControl Content Database, and responds with the category ID of the queried URL.

The SurfControl CPA Server is installed on a separate server that must be accessible from the Cisco SCE platform. Details of the installation are not within the scope of this document.

The Content Filtering CLI

Use the Cisco SCE platform Command-Line Interface (CLI) to configure and monitor content filtering using SurfControl CPA. For more information about the Cisco SCE platform CLI, see the .

CPA Client CLI Commands

The commands listed here are explained in the following section.

- Use the following CLI line interface configuration commands in line interface configuration mode to configure the Cisco CPA client:

[**[no]**] **cpa-client cpa-client destination** *address* [**port** *port*] **cpa-client retries** *number_of_retries*
For details on entering the line interface configuration mode, see Entering Line Interface Configuration Mode , on page 231 section).

- Use the following CLI command in EXEC mode to monitor the status of the Cisco CPA client:**show interface LineCard** *slot* **cpa-client**

Description of CPA Client CLI Commands

Table 8: CPA Client CLI Commands

Command	Description	Default Value
[no] cpa-client	Enables or disables the CPA client	Disabled
cpa-client destination <address> [**port** <port>]	Enables the CPA client and sets the CPA server IP address and port	• Address—not defined • Port—9020

Command	Description	Default Value
cpa-client retries <number_of_retries>	Sets the number of retries to send to the CPA server	3
show interface LineCard <slot> **cpa-client**	Monitors the CPA client status (See the following table)	—

Table 9: CPA Client: Monitored Parameters

Parameter	Description
Mode	Enabled or disabled
CPA Address	—
CPA Port	—
CPA Retries	—
Status	(If enabled) Active or error (and last error description)
Counters	• Number of successful queries • Number of queries that failed because of no server response • Number of pending queries • Rate of queries per second (average over the last 5 seconds)
Timestamps	• CPA started • Last query • Last response • Last error

Configuring the RDR Formatter

To enable the RDR formatter to issue HTTP categorization requests, configure the RDR formatter on the Cisco SCE platform.

Procedure

Step 1

Step 2 Run the appropriate CLI commands on Cisco SCE platform.

Example:
#>**RDR-formatter destination** *127.0.0.1* **port** *33001* **category number** *4* **priority** *100*

What to Do Next

Entering Line Interface Configuration Mode

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

Procedure

Step 1 At the Cisco SCE platform CLI prompt (SCE#), type configure .

Step 2 Press Enter.
The SCE(config)# prompt appears.

Step 3 Type **interface LineCard 0**.

Step 4 Press Enter.
The SCE(config if)# prompt appears.

Managing Content Filtering Settings

Applying HTTP URL content filtering requires the following steps in the Service Configuration Editor:

Procedure

Step 1 Import the content filtering configuration file into your service configuration.
By default, Cisco SCA BB creates a separate flavor (of type HTTP Content Category) for each content category and a service element for each new flavor. A new top-level service, “HTTP Browsing with Categories”, is created, comprising these service elements.

Step 2 Create new services and map the new category flavors to them.
Step 3 Create additional rule entries for ClickStream services for each flavor.
Step 4 Configure ClickStream Services with the HTTP Browsing services for optimal HTTP content filtering.
Step 5 Add content filtering rules to existing packages or create new packages that include content filtering rules.
Step 6 Enable content filtering for selected packages.
Step 7 Apply the service configuration.

What to Do Next

Importing Content Filtering Categories

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



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

Procedure

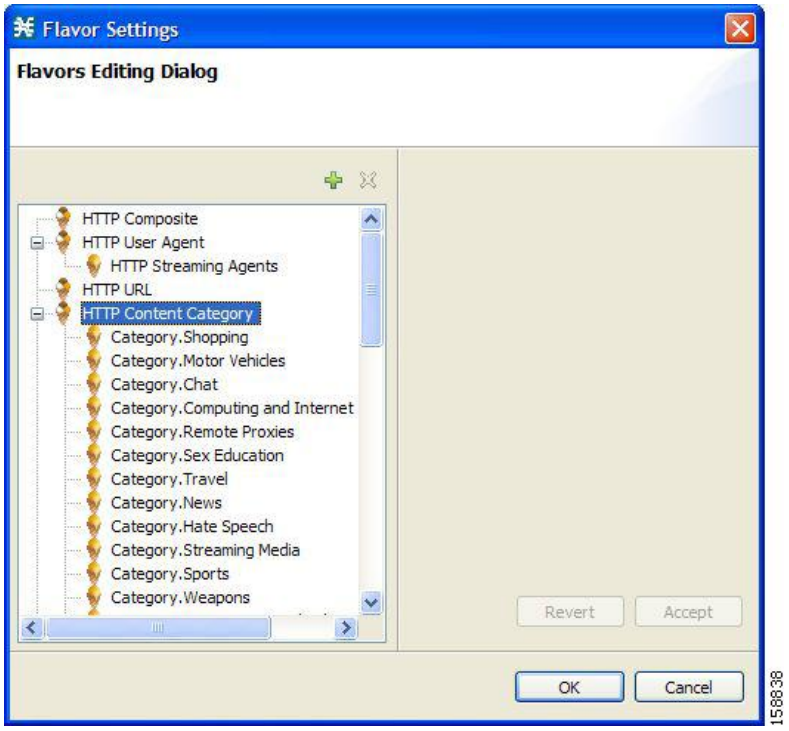
Step 1 Unzip the installation package.
Step 2 Open the URL Filtering subfolder.

What to Do Next

HTTP Content Category Flavors

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

Figure 159: Flavor Settings

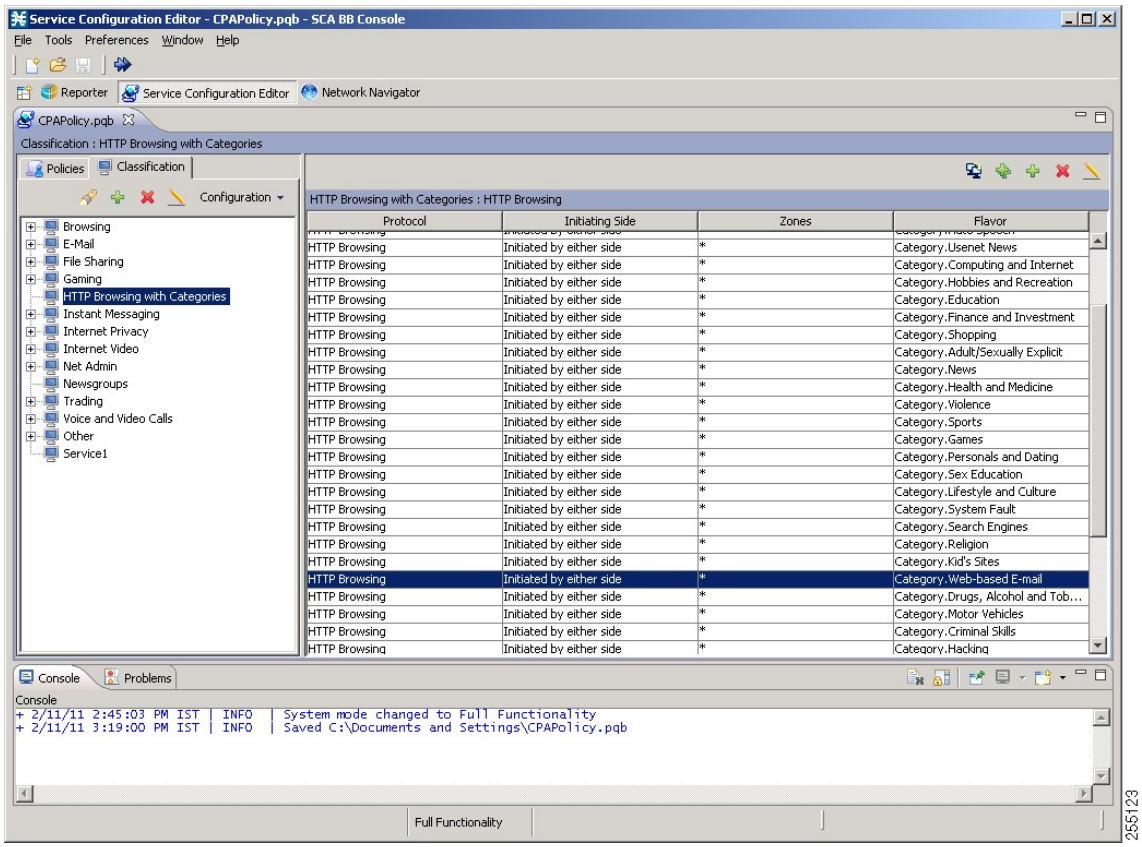


You can create additional HTTP Content Category Flavors that include two or more content categories. (See Adding Flavors, on page 218 section.)

HTTP Browsing with Categories Service Elements

By default, Cisco SCA BB creates a service element for each flavor created when importing the XML file. A new top-level service, HTTP Browsing with Categories, is created, comprising these service elements.

Figure 160: Service Configuration Editor



Note To view this new service, you must save and close the service configuration and then reopen it.

Importing Content Filtering Categories Using the Import Dialog Box

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

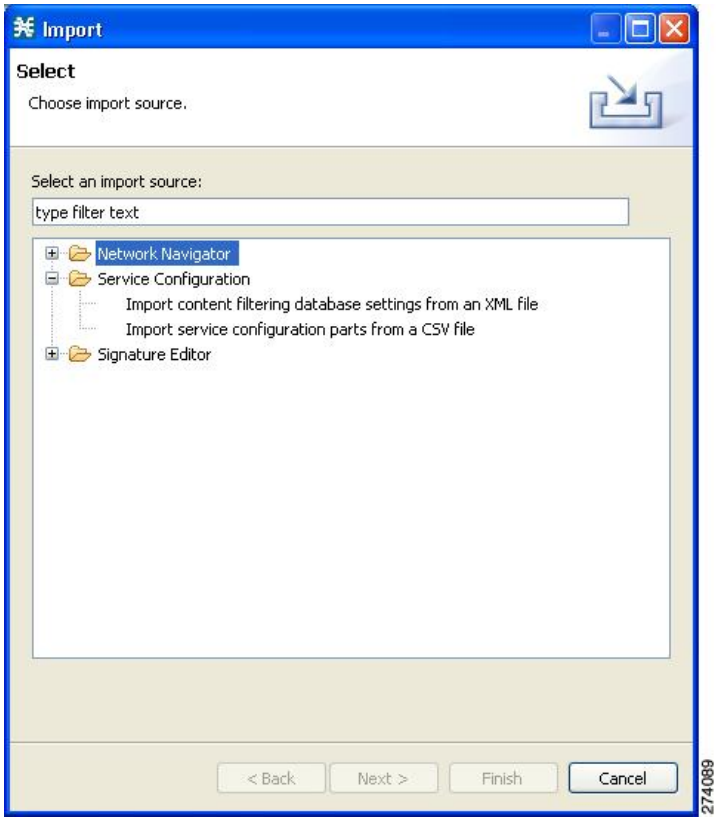
This procedure explains how to import using the File > Import menu option.

Note This is equivalent to the following procedure.

Procedure

Step 1 From the Console main menu, choose File > Import .
The Import dialog box appears.

Figure 161: Import

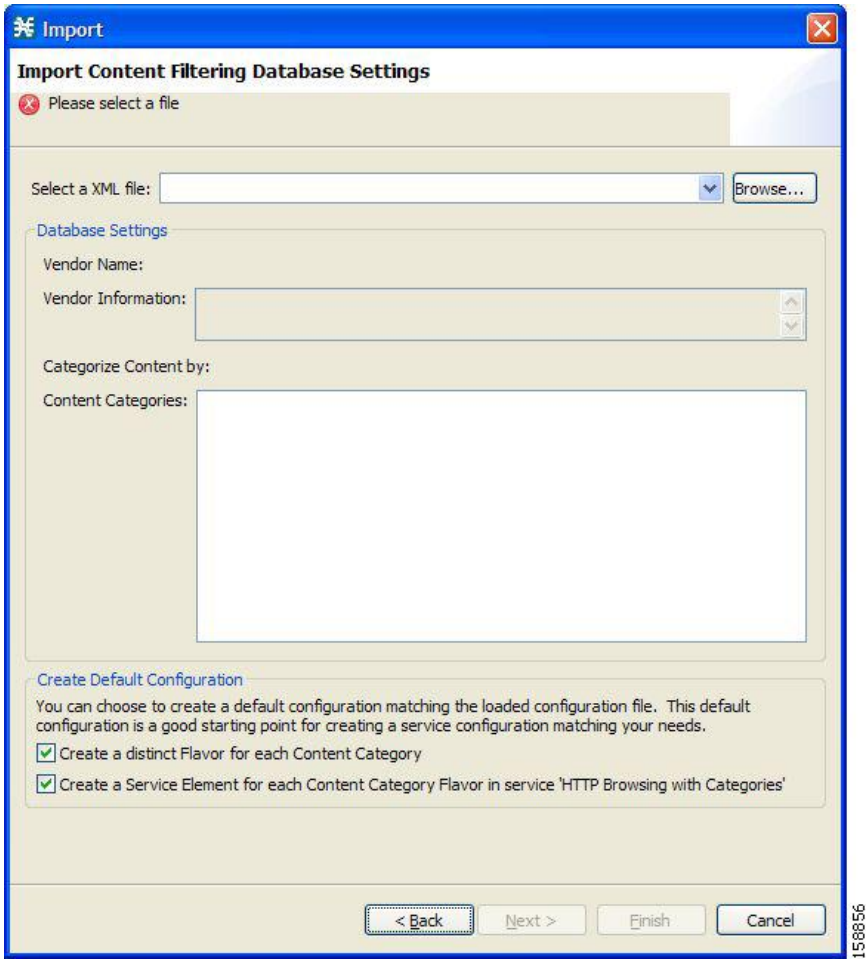


Step 2 From the import source list, select Import content filtering database settings from an XML file.

Step 3 Click Next.

The Import Content Filtering Database Settings dialog box appears.

Figure 162: Import Content Filtering Database Settings



Step 4 Click the Browse button next to the Select an XML file field.
An Open dialog box appears.

Step 5 Browse to the folder containing the file to import, and select it.
Note For CPAof SurfControl, the file is named surfcontrol.xml.

Step 6 Click Open to select the file.
The Open dialog box closes.

Information about the content of the XML file is displayed in the Database Settings pane of the Import Content Filtering Database Settings dialog box.

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

By default, Cisco SCA BB creates a service element for each flavor created in the previous Step. A new top-level service, HTTP Browsing with Categories, is created, comprising these service elements.

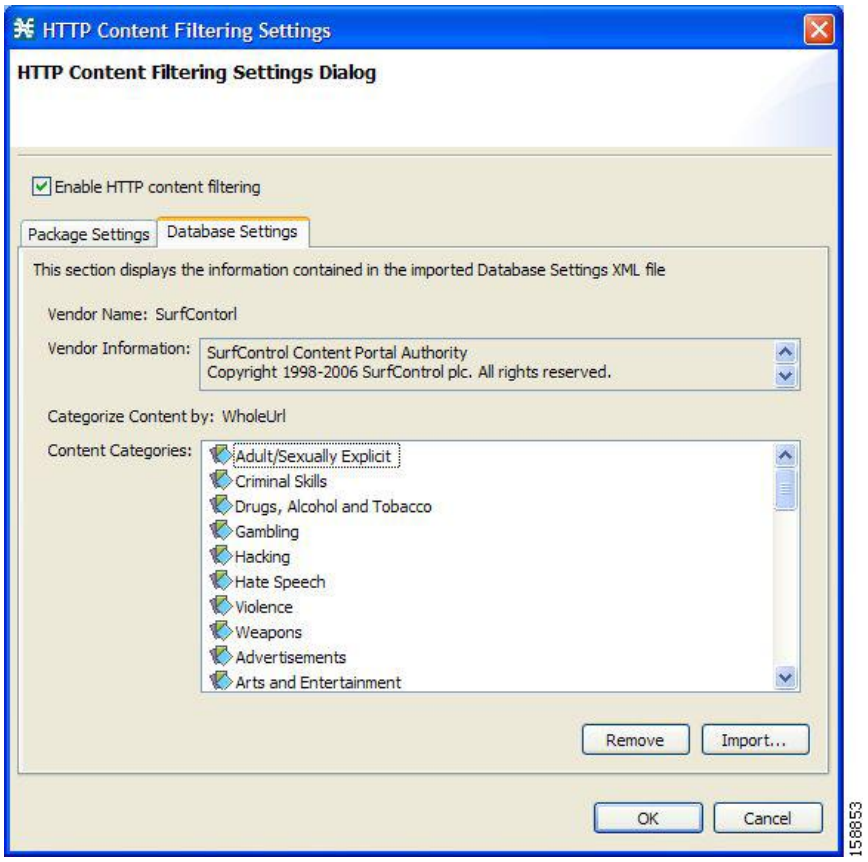
Step 7 (Optional) To disable the default behavior of creating a separate flavor for each content category, uncheck the Create a distinct Flavor for each Content Category check box.
Note It is recommended that you do not disable this option.

Step 8 (Optional) To disable the default behavior of creating service element for each flavor, uncheck the Create a Service Element for each Content Category Flavor in Service 'HTTP Browsing with Categories' check box.
Note It is recommended that you do not disable this option.

Step 9 Click Finish.
The Import Content Filtering Database Settings dialog box closes.

Information from the imported file is displayed in the Database Settings tab of the HTTP Content Filtering Settings dialog box.

Figure 163: HTTP Content Filtering Settings



Step 10 Click OK.
The HTTP Content Filtering Settings dialog box closes.

Importing Content Filtering Categories Using the HTTP Content Filtering Settings Dialog Box

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

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

Note This is equivalent to the Importing Content Filtering Categories Using the Import Dialog Box, on page 234 procedure.

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Content Filtering . The HTTP Content Filtering Settings dialog box appears.

Step 2 Click the Database Settings tab.
The Database Settings tab opens.

Step 3 Click Import.
The Import Content Filtering Database Settings dialog box appears.

Step 4 Click the Browse button next to the Select an XML file field.
An Open dialog box appears.

Step 5 Browse to the folder containing the file to import, and select it.
Note For the CPA of SurfControl, the file is named surfcontrol.xml.

Step 6 Click Open to select the file.
The Open dialog box closes.

Information about the content of the XML file is displayed in the Database Settings pane of the Import Content Filtering Database Settings dialog box.

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

By default, Cisco SCA BB creates a service element for each flavor created in the previous Step. A new top-level service, HTTP Browsing with Categories, is created, comprising these service elements.

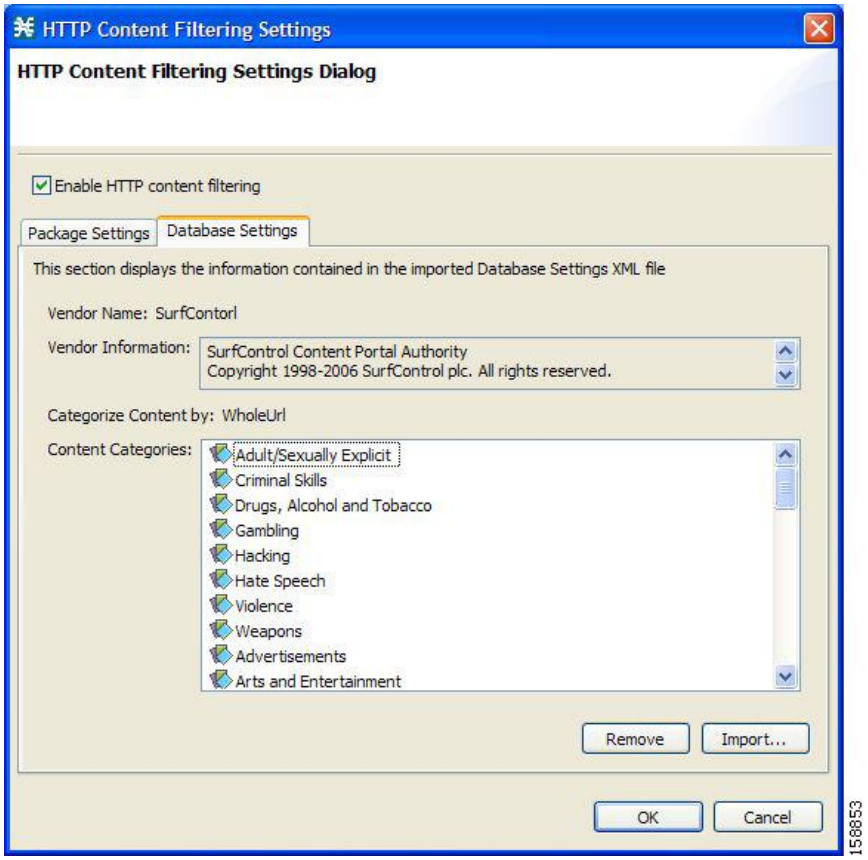
Step 7 (Optional) To disable the default behavior of creating a separate flavor for each content category, uncheck the Create a distinct Flavor for each Content Category check box.
Note It is recommended that you do not disable this option.

Step 8 (Optional) To disable the default behavior of creating a service element for each flavor, uncheck the Create a Service Element for each Content Category Flavor in Service 'HTTP Browsing with Categories' check box.
Note It is recommended that you do not disable this option.

Step 9 Click Finish.
The Import Content Filtering Database Settings dialog box closes.

Information from the imported file is displayed in the Database Settings tab of the HTTP Content Filtering Settings dialog box.

Figure 164: HTTP Content Filtering Settings



Step 10 Click OK.
The HTTP Content Filtering Settings dialog box closes.

Enabling Content Filtering

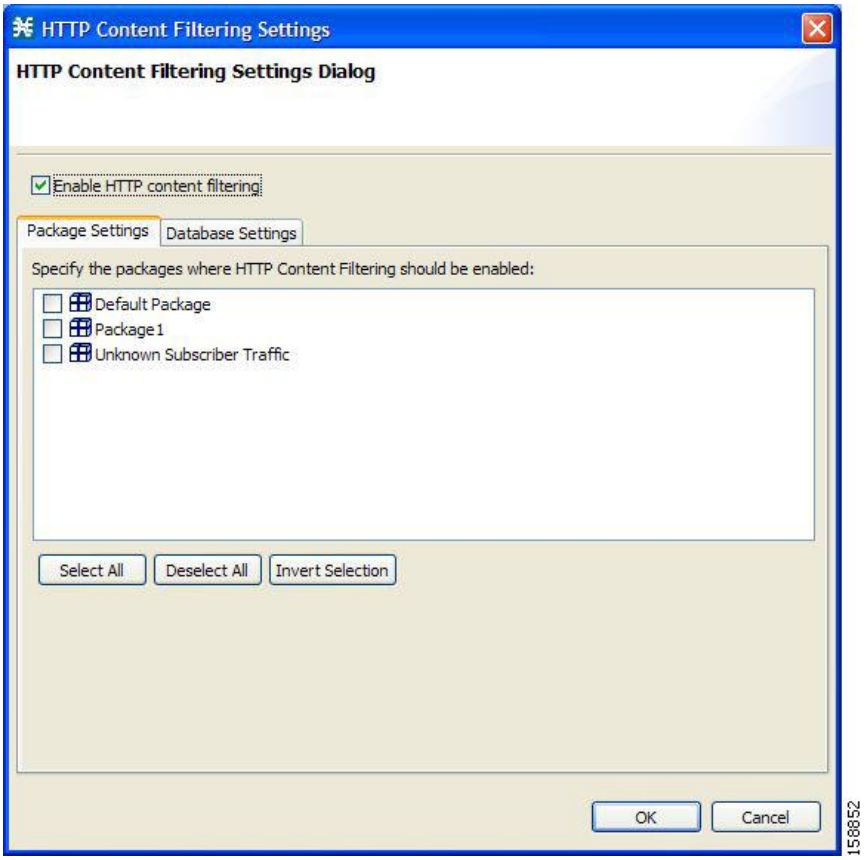
You can specify the packages where content filtering is enabled. For packages where content filtering is disabled, HTTP flows are classified normally.

Procedure

Step 1 From the Classification tab in the left pane, choose **Configuration** > **Classification** > **Content Filtering**.
The HTTP Content Filtering Settings dialog box appears.

The Package Settings tab displays a list of all packages defined for the current service configuration.

Figure 165: HTTP Content Filtering Settings



Step 2 Check the Enable HTTP content filtering check box.

Step 3 Check the check box next to each package for which content filtering is to be applied.

Step 4 Click OK.
The HTTP Content Filtering Settings dialog box closes.

Viewing Content Filtering Settings

You can view whether content filtering is enabled and to which packages content filtering is applied, and information about the content filtering vendor and the content categories of the vendor.

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Content Filtering .
The HTTP Content Filtering Settings dialog box appears.

The Package Settings tab displays a list of all packages defined for the current service configuration, and shows for which packages content filtering is enabled.

Step 2 Click the Database Settings tab.
The Database Settings tab opens.

This tab displays information about the content filtering vendor and the content categories of the vendor.

Step 3 Click OK .
The HTTP Content Filtering Settings dialog box closes.

Configuring Content Filtering

While configuring Content Filtering, you must enter the ClickStream-New Page and ClickStream-New Site services along with HTTP Browsing protocol services for optimal HTTP content filtering.

The term ClickStream refers to all events generated by user clicks, including enter. If configured, Cisco SCE identifies the HTTP transactions on the flows that were initialized due to direct user actions such as click on a link, enter a URL in the browser address bar and press enter.

Procedure

Step 1 Open Cisco SCA BB Service Configuration Editor with the default content filtering file (PQB).

Step 2 Add a new service Service1.

Step 3 Verify that you do not have duplicate service elements. Cisco SCA BB does not allow duplicate service elements.

Step 4 Move the desired service element from HTTP Browsing with Categories to Service1.

Step 5 In Service1 , add a service element using protocol ClickStream–New Page and with the same Flavor selected in Step 4.

Step 6 In Service1, add a service element using protocol ClickStream–New Site and with the same Flavor selected in Step 4.

Step 7 Save the service configuration file (PQB).

Step 8 Use the service to create rules in the desired package.

Example for How to Configure Content Filtering for Web Based E-mail

To configure content filtering for Web Based E-mail, complete the following steps:

Procedure

Step 1 Open Cisco SCA BB Service Configuration Editor with the default content filtering file (PQB).

Step 2 Add a new service Service1.

Step 3 Move the service element Category.Web-based E-mail from HTTP Browsing with Categories to Service1.

Step 4 In Service1 , add a service element using protocol ClickStream–New Page and Flavor Category.Web-based E-mail .

Step 5 In Service1 , add a service element using protocol ClickStream–New Site and Flavor Category.Web-based E-mail .

Step 6 Save the service configuration file (PQB) and use the service to create rules in the desired package.

Removing Content Filtering Settings

You can remove all content filtering settings at any time.

Removing the settings:

- Removes content category flavor items from flavors
- Deletes all the content category flavor items
- Disables content filtering

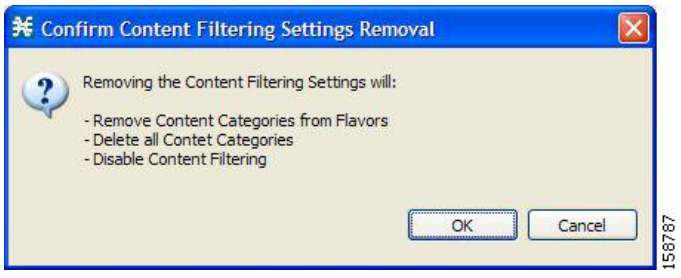
Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > Content Filtering .
The HTTP Content Filtering Settings dialog box appears.

Step 2 Click the Database Settings tab.
The Database Settings tab opens.

Step 3 Click Remove .
A Confirm Content Filtering Settings Removal dialog box appears.

Figure 166: Confirm Content Filtering Settings Removal



Step 4 Click OK.
All content filtering settings are removed.

Vendor Name, Vendor Information, and Content Categories are deleted from the HTTP Content Filtering Settings dialog box.

Step 5 Click OK.
The HTTP Content Filtering Settings dialog box closes.

- Generic Protocols—Generic IP, Generic TCP, and Generic UDP protocols, used for transactions that are not specifically mapped to a protocol by any other protocol type.
- IP Protocols—Protocols (such as ICMP), other than TCP and UDP protocols, identified according to the IP protocol number of the transaction.
- Port-Based Protocols—TCP and UDP protocols, classified according to their well-known ports. The default service configuration includes more than 750 common port-based protocols.
- Signature-Based Protocols—Protocols classified according to a Layer 7 application signature. Includes the most common protocols, such as HTTP and FTP, and a large group of popular P2P protocols.
- P2P Protocols—Peer-to-peer file-sharing application protocols classified according to a Layer 7 application signature.
- VoIP Protocols—Voice-over-IP application protocols classified according to a Layer 7 application signature.
- SIP Protocols—Protocols classified according to a Layer 7 application signature that is SIP or has SIP characteristics.
- Worm Protocols—Protocols classified according to a Layer 7 application signature that is based on traffic patterns of Internet worms.
- Packet Stream Pattern Based Protocols—Protocols classified according to a Layer 7 application signature that is based on the pattern of the packet stream (for example, the stream's symmetry, average packet size, and rate) rather than on the packet's payload content.
- Unidirectionally Detected Protocols—Protocols having a unidirectional signature.

Note Some protocols belong to more than one category. In particular, all predefined P2P, VoIP, SIP, Worm, and Packet Stream Pattern-Based Protocols are also defined as Signature-Based Protocols.

Step 6 From the Classification tab in the left pane, choose Configuration > Classification > Protocols .
The Protocol Settings dialog box appears.

Step 7 From the drop-down list in the Protocols tab, select the type of protocol to display.
The protocols of the selected type appear in the Protocols tab.

Step 8 Click Close .
The Protocol Settings dialog box closes.

Note The setting in the drop-down list is not saved. The next time you open the Protocol Settings dialog box, all protocols are displayed.

OS Fingerprinting Overview

Cisco SCE detects the operating system (OS) used by a subscriber by using the passive OS Fingerprinting. In passive OS fingerprinting, TCP and IP header received from target host is analyzed to identify the OS.

Cisco SCE uses OS fingerprinting signatures to identify the subscriber OS. By default, Cisco SCOS contains a signature file that contains a default set of OS. Details of unknown OS may be added to the signature files using the Cisco SCA BB Console.

Cisco SCE also determines whether the subscriber is behind a NAT and whether the same subscriber is connecting using multiple OS. If multiple OS is detected for the same subscriber, Cisco SCE considers the subscriber as using a NAT.

From the Cisco SCA BB Console, you can also configure Cisco SCE to send the OS information of the subscriber in Gx messages.

Limitations:

- OS information is available only for logged-in or active subscribers.
- The signature database is built based on the default settings used by various OS. If the user changes the default parameters like TCP window size through registries, it would not be possible or may lead to wrong classification of the OS.
- If the subscriber has only one flow, then OS type is be detected. Subscribers that have only UDP flows are not detected
- If all users behind a NAT use the same OS, it will not be possible to identify NAT.
- If a subscriber runs multiple OS using VMWare, it may be detected as NAT even though the subscriber is not in a NAT environment
- OS finger printing is not done continuously for any subscriber. So, if a subscriber changes OS or moves to a NAT environment during the time when he is not sampled, OS Information and NAT cannot be detected.

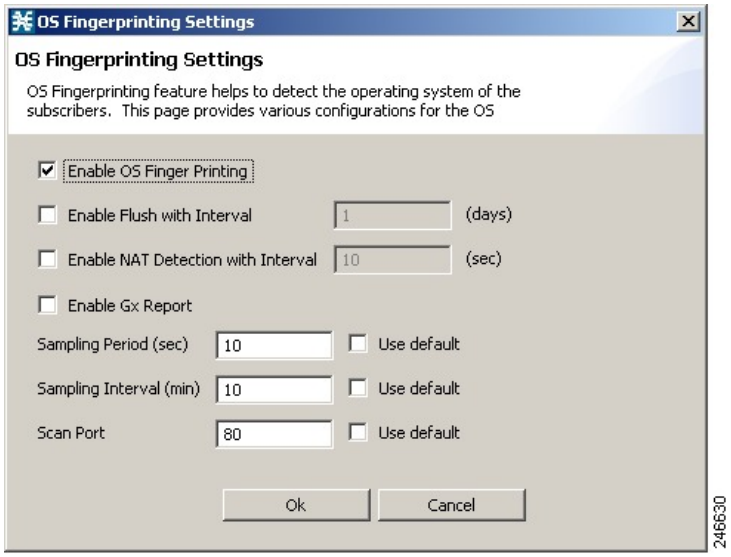
Enabling OS Fingerprinting

Procedure

Step 1 In Service Configuration Editor, select Configuration > OS Finger Print... .
The OS Fingerprinting Settings dialog box appears.

Step 2 Check the Enable OS Finger Printing check box.

Figure 167: OS Finger Print Settings Dialog Box



Step 3 Enable Flush with Interval—Check the Enable Flush with Interval check box and enter the interval in days to configure the interval after which the OS information will be reset.

Step 4 (Optional) Enable NAT Detection with Interval—Check the Enable NAT Detection with Interval check box and enter the interval in seconds to configure the time period with-in which multiple OS detection will trigger NAT identification. Default value is 10 seconds.

Step 5 (Optional) Enable Gx Report—Check the Enable Gx Report check box to enable Gx Reports.

Step 6 Configure Sampling Period (sec)—Configure how long flows from a subscriber will finger-printed. Default is 10 seconds. Check the Use default check box to use the default period.

Step 7 Configure Sampling Interval (min)—Enter the time in minutes to configure the frequency at which flows will be finger-printed. Default is 10 minutes. Check the Use default check box to use default interval.

Step 8 (Optional) Scan Port—Enter a value for Scan Port used for opening OS finger printing flows. Check the Use default check box to use the default port—port 80—for the flows. Ports 20, 21, 69, and 5060 are not allowed.

Step 9 Click Ok.

What to Do Next

Note After enabling OSFP in Cisco SCE using Cisco SCA BB console, enable the OSFP Reports in Cisco Service Control Collection Manager. For details on enabling the OSFP Reports in Cisco Service Control Collection Manager, see the Cisco Service Control Collection Manager User Guide.

Installing OS Fingerprinting Signatures

Procedure

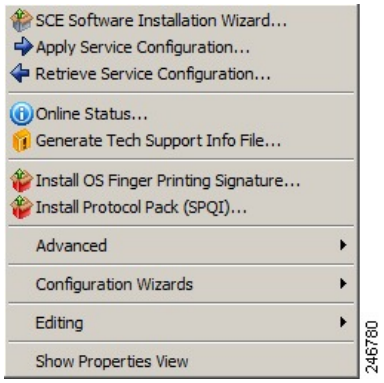
Step 1 (Optional) Using Network Navigator, add the device on which you need to install the signatures.

Step 2 Enable OS Fingerprinting.
See the Enabling OS Fingerprinting, on page 244 section.

Step 3 Apply the configuration to the device.

Step 4 In the Site Manager tree, right-click a Cisco SCE device.
A popup menu appears.

Step 5 From the menu, select **Install OS Finger Printing Signature...** .



246780.jpg

The Password Management dialog box appears. For details on password management, see the Password Management , on page 112 section.

Step 6 Enter the User Name and Password, and click **Update**.
The Update OSFP Signature window appears.

Step 7 Enter the path to signature file in the Select OSFP Signature File field or Browse to the signature file.

Step 8 Click Finish.
A confirmation message appears in the Console.

Viewing Subscriber OS Information

Procedure

Step 1 Enable OS Fingerprinting. See the Enabling OS Fingerprinting, on page 244 section.

Step 2 Apply the configuration to the device.

Step 3 From Subscriber Manager, view the Subscriber list..

Step 4 Right-click on the device, and select View Online Status .

The online status of the subscriber appears near the console panel with the OS information. The OS Fingerprinting is available for Anonymous Groups through Anonymous Group Manager GUI Tool.

Disabling OS Fingerprinting

Procedure

Step 1 In the Service Configuration Editor, select **Configuration** > **OS Finger Print...** .
The OS Finger Printing Settings dialog box appears.

Step 2 Uncheck the **Enable OS Finger Printing** check box.

The OS Fingerprinting CLI

Use the following CLI command in EXEC mode to monitor the OS details of the subscriber:

show os-fingerprinting subscriber-name
In this example, Cisco SCE has detected a NAT and behind the NAT two OS. One is iOS with an index number 65 and another OS that is not known to Cisco SCE:

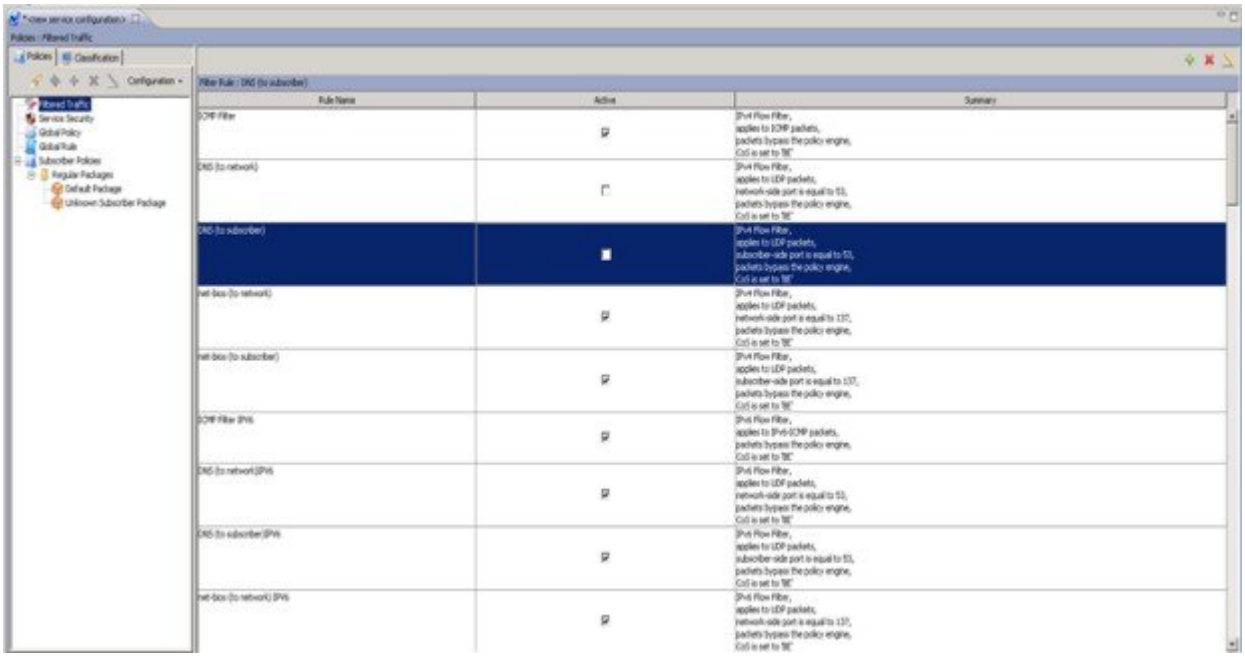
Configuring Policy for DNS Assisted Classification

By default, the DNS traffic is bypassed via the default flow-filters configured in the policy. We need to disable **DNS(to network)** and **DNS(to subscriber)** flow-filters and enable first packet classification for DNS traffic, since the packets per DNS-flow are very less and in most of the cases there are only two packets; For example, Request and Response

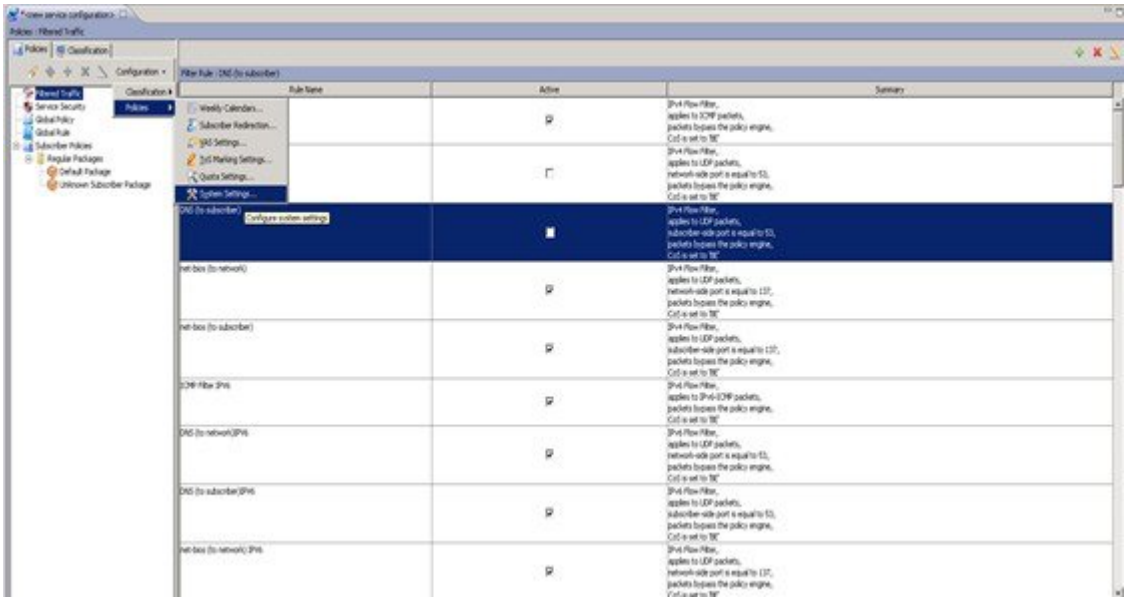
To configure Policy for DNS Assisted Classification, follow the below procedure:

Procedure

Step 1 In the existing service configuration policy, select **Policy** tab and the select **Filtered Traffic** from the left navigation pane.



Step 2 Disable the **DNS(to network)** and **DNS(to subscriber)** check boxes in the active pane.

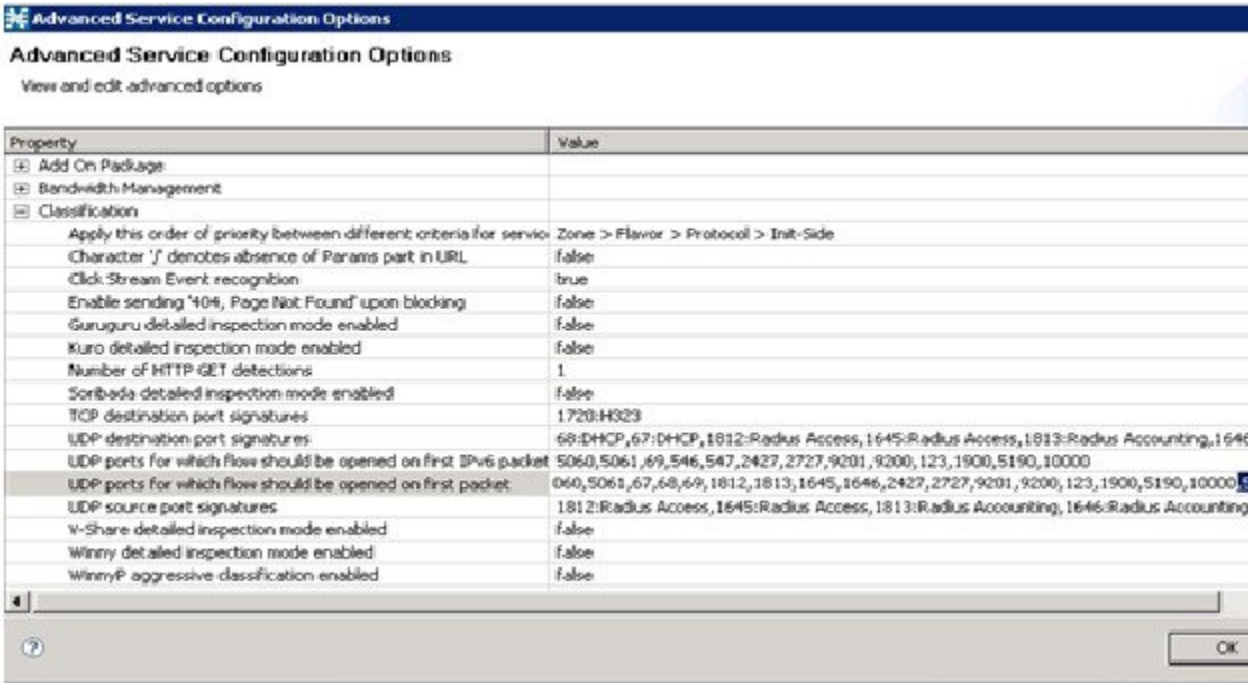


Step 3 Select **Configuration > Policies > System Settings**… from the **Policies :Filtered Traffic** window. The **System Settings** dialog box appears.



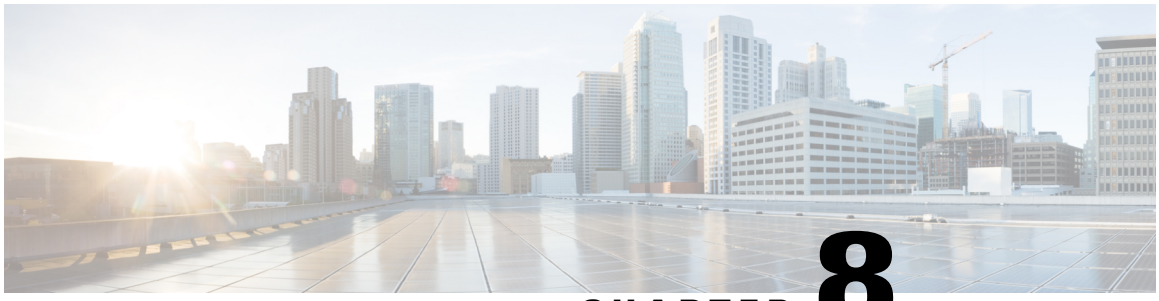
Step 4 Select **Advanced Options** tab and click **Advanced Service Configuration Options ...** The **Advanced Service Configuration Options** window appears.

Step 5 Under **Classification** properties, add a value 53 to the **UDP ports for which flow should be opened on first packet** option.



Step 6 Click **Ok** to close **Advance Service Configuration Options** window.

Step 7 Click **Ok** to close **System Settings** dialog box.
Apply the Service configuration policy to the SCE.



CHAPTER 8

Traffic Accounting and Reporting Using the Service Configuration Editor

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

Traffic Accounting and Reporting is the second step in creating a Cisco SCA BB service configuration. This chapter consists of these sections:

- Usage Counters, page 251
- Raw Data Records, page 252
- NetFlow Records , page 252
- Managing RDR Settings, page 252

Usage Counters

The Cisco SCA BB collects and maintains various network metrics (such as volume and number of sessions) per service. This accounting takes place per subscriber, per group of subscribers (package or group of packages), and for the entire link.

Service Usage Counters

The system uses the service usage counters to generate data about the total use of each service. A service can use either its own usage counters, or the usage counters of its parent service. For example, in the default service configuration the SMTP and POP3 services share the E-Mail service usage counters. Service hierarchy determines the assignment of services to usage counters. For details on how to configure the service hierarchy, see Editing Services , on page 165 section.

Package Usage Counters

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

The system uses the package usage counters to generate data about the total use of each package. A package can use either its own usage counters, or the usage counters of its parent package. The package hierarchy determines the assignment of packages to usage counters. For details on how to configure the package hierarchy, see Setting Advanced Package Options, on page 322 section.

Raw Data Records

Cisco Service Control Engine (Cisco SCE) platforms generate and transmit Raw Data Records (RDRs) that contain information relevant to the service provider. These RDRs contain a wide variety of information and statistics, depending on the configuration of the system.

- All RDR data is based on Layer 3 volume.
- RDRs are not generated for filtered traffic. For details, see Traffic Flow Filtering, on page 399 section.

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

NetFlow Records

- You enable and disable the export of NetFlow records using the CLI.

  You can export records per supported RDR type. The data in the following RDR types can be exported using NetFlow:

  - Subscriber Usage RDR
  - Package Usage RDR
  - Link Usage RDR
  - Zone Usage RDR

- The NetFlow records can be sent to more than one collection device.
- NetFlow records can be generated concurrently with RDRs.

Managing RDR Settings

This section explains how to configure the generation of the different types of RDRs.

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

- RDRs are not generated for filtered traffic (see Traffic Flow Filtering, on page 399 section).
- All RDR data is based on Layer 3 volume.

The RDR Settings Dialog Box

The RDR Settings dialog box allows you to control the generation of RDRs for an entire service configuration. This dialog box contains seven tabs:

- Usage RDRs tab—Allows you to enable the generation each type of Usage RDR, and define their generation intervals

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



Note Media Flow RDRs and Malicious Traffic Periodic RDRs are enabled and configured in the Advanced Service Configuration Options, on page 435.

Managing Usage RDRs

The five types of Usage RDRs contain data about total usage of all services included in a service usage counter:

- Link Usage RDRs—For the entire link
- Package Usage RDRs—For all subscribers to a particular package
- Subscriber Usage RDRs—For a particular subscriber
- Virtual Links Usage RDRs—For a particular group of virtual links
- Zone Usage RDRs—For the entire zone

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

By default, all four types of Usage RDRs are enabled. (Virtual Links Usage RDRs are enabled by default only if Virtual Links mode was enabled when you created the service configuration.)



Note Usage RDRs are not generated for blocked sessions. A session is blocked if the service to which the session is mapped is blocked for the package for this subscriber (see Defining Per-Flow Actions for a Rule , on page 335 section), or if the subscriber has exceeded the allowed quota for this service (see Quota Management, on page 360“Managing Quotas” section on page 9-90).

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in Cisco Service Control Application for Broadband Reference Guide :

- Link Usage RDR
- Package Usage RDR

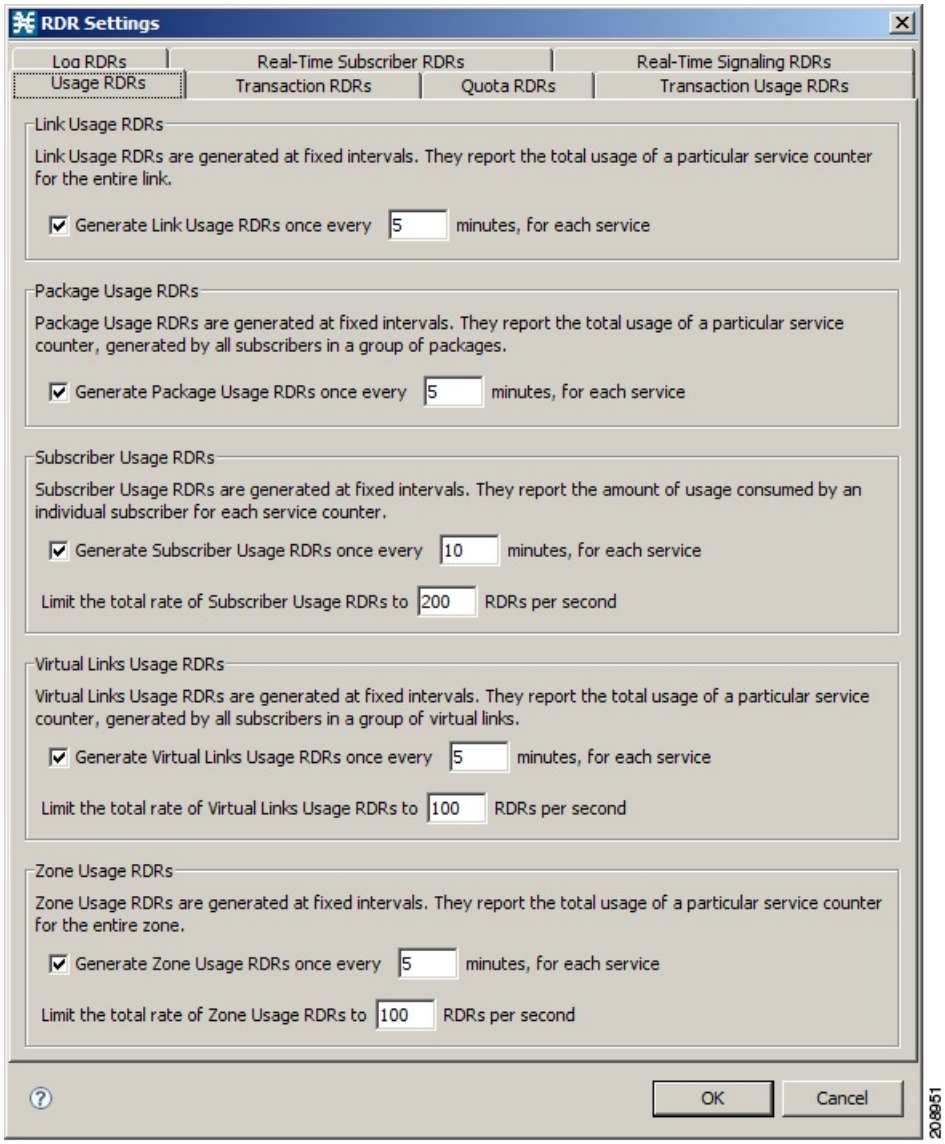
- Subscriber Usage RDR
- Virtual Link Usage RDR
- Zone Usage RDR

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > RDR Settings .

The RDR Settings dialog box appears.

Figure 168: RDR Settings



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.

Note The interval rate entered in the Subscriber Usage RDR, Virtual Links Usage RDR, and Zone Usage RDR fields is divided by the number of traffic processors present in the Cisco SCE and the same gets updated in the respective tunable.

Step 4 To limit the generation rate of Subscriber Usage RDRs, enter the maximum number of Subscriber Usage RDRs to be generated per second in the Limit the Total Rate of Subscriber Usage RDRs field.

Step 5 Click OK.
The RDR Settings dialog box closes.

The new configuration for the generation of Usage RDRs is saved.

Managing Transaction RDRs

Each Transaction RDRs contain data about a single network transaction. The Cisco SCE platform can generate Transaction RDRs for selected service types. You can use these RDRs, for example, to generate statistical histograms that help understand the traffic traversing the network.

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

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

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the “Transaction RDR” section in the Cisco Service Control Application for Broadband Reference Guide.

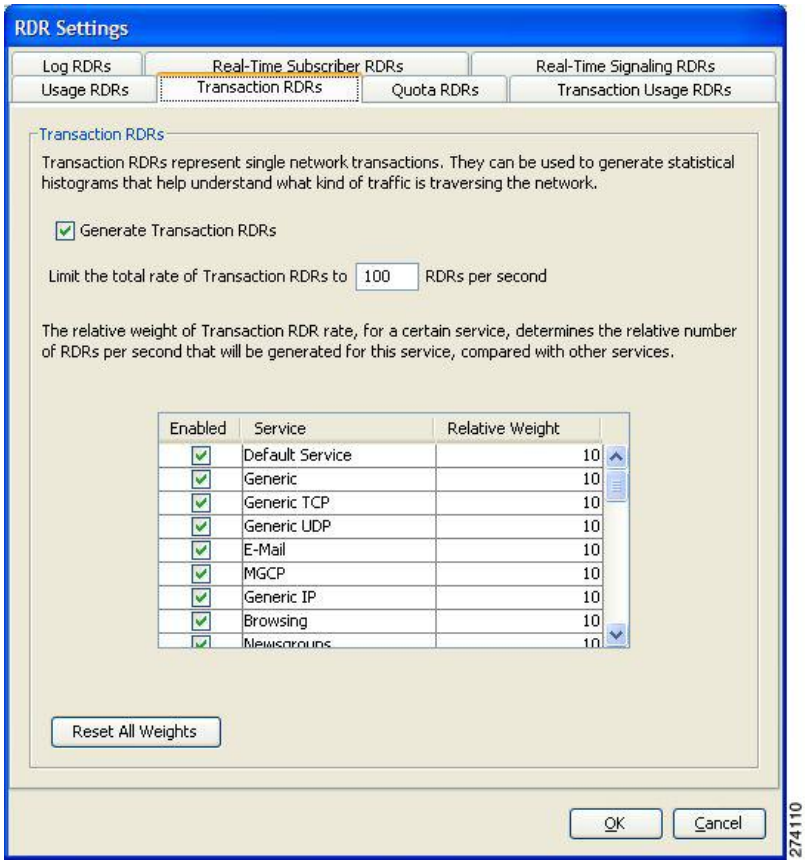
Procedure

Step 1 From the Classification tab in the left pane, choose **Configuration** > **Classification** > **RDR Settings** .
The RDR Settings dialog box appears.

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

The Transaction RDRs tab opens.

Figure 169: Transaction RDRs Tab



Step 3 To enable the generation of Transaction RDRs, check the **Generate Transaction RDRs** check box.
To disable the generation of Transaction RDRs, uncheck the **Generate Transaction RDRs** check box.

Step 4 To change the maximum generation rate for Transaction RDRs, enter the desired rate in the Limit the Total Rate of Transaction RDRs field.

Step 5 To disable the generation of Transaction RDRs for a selected service, uncheck the Enabled check box next to the service name.

Step 6 To set the relative weight for a selected service, double-click in the appropriate cell in the Relative Weight column, and enter the desired weight.

Step 7 Click **OK**.
The RDR Settings dialog box closes.

The new configuration for the generation of Transaction RDRs is saved.

Managing Quota RDRs

Each Quota RDR contains data for a single subscriber. There are four types of Quota RDRs:

- Quota Breach RDRs—Generated when a quota breach occurs, that is, when services that try to consume from a depleted quota bucket.
  A breached service is handled according to its breach-handling settings. For example, when the quota for a service is consumed, you can block its flows.
- Remaining Quota RDRs—Generated as quota is consumed, but only if a bucket state has change since the last Remaining Quota RDR was generated.
- Quota Threshold Breach RDRs—Generated when the remaining quota in a bucket falls below a threshold. External systems can treat this RDR as a quota request and provision the subscriber with an additional quota before the bucket is depleted.
- Quota State Restore RDRs—Generated when a subscriber is introduced. When a subscriber logs out, their remaining quota is stored in the Cisco Service Control Subscriber Manager (SM). When the subscriber logs in again, this quota is restored from the SM.

You can enable or disable the generation each type of Quota RDR and define the rate of generation of these RDRs.

- For Remaining Quota RDRs, you can set the generation interval, and limit the generation rate (advisable when there are a large number of subscribers).
- For Quota Threshold RDRs, you can configure the threshold.

By default, all Quota RDRs are disabled.

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in the Cisco Service Control Application for Broadband Reference Guide:

- Quota Breach RDR
- Remaining Quota RDR
- Quota Threshold Breach RDR
- Quota State Restore RDR

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > RDR Settings .
The RDR Settings dialog box appears.

Step 2 Click the Quota RDRs tab.

The Quota RDRs tab opens.

Figure 170: Quota RDRs Tab



Step 3 To enable the generation of Quota Breach RDRs, check the Generate Quota Breach RDRs check box.

Step 4 To enable the generation of Remaining Quota RDRs, check the Generate Remaining Quota RDRs check box.

Step 5 To change the generation interval of Remaining Quota RDRs, in the Generate Remaining Quota RDRs field, enter the interval in minutes between each generation of the RDR.

Step 6 To limit the maximum generation rate of Remaining Quota RDRs, in the Limit the Total Rate of Remaining Quota RDRs field, enter the maximum number of Remaining Quota RDRs to be generated per second.

Step 7 To enable the generation of Quota Threshold RDRs, check the Generate Quota Threshold RDRs check box.

Step 8 To change the Threshold for Quota Threshold RDRs, in the Generate Quota Threshold RDRs field, enter the threshold for which Quota Threshold RDRs are generated.

Step 9 To enable the generation of Quota State Restore RDRs, check the Generate Quota State Restore RDRs check box.

Step 10 Click OK.

The RDR Settings dialog box closes.

The new configuration for the generation of Quota RDRs is saved.

Managing Transaction Usage RDRs

Transaction Usage RDRs are generated for all transactions of selected packages or for selected services per package. Each Transaction Usage RDR contains data about a single network transaction. You can use these RDRs, for example, to build detailed usage logs for specific services and subscribers for transaction-based billing.

Caution Generating and collecting an RDR for each transaction can compromise performance. Enable Transaction Usage RDR generation only for services and packages that must be monitored or controlled.

You can select the packages and services for which Transaction Usage RDRs are generated. The following RDRs are also generated for these packages and services:

- HTTP Transaction Usage RDR
- RTSP Transaction Usage RDR
- VoIP Transaction Usage RDR

By default, no Transaction Usage RDRs are generated.

Note Media Flow RDRs are enabled using the Advance Service Configuration Options. When enabled, Media Flow RDRs are generated at the end of every SIP and Skype media flow. You can use the Media Flow RDRs to distinguish between SIP voice and video calls. For details on enabling Media Flow RDRs, see Editing Advanced Service Configuration Options , on page 443 section.

For details on the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in the Cisco Service Control Application for Broadband Reference Guide :

- Transaction Usage RDR
- HTTP Transaction Usage RDR
- RTSP Transaction Usage RDR
- VoIP Transaction Usage RDR

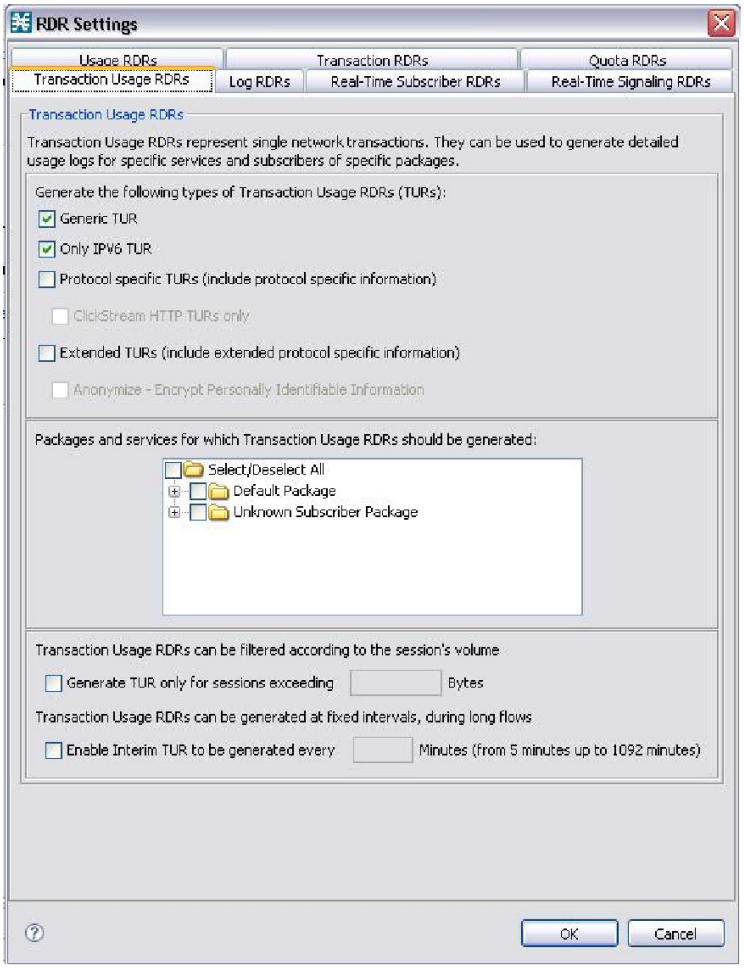
Procedure

Step 1 From the Classification tab in the left pane of Service Configuration Editor window, choose Configuration > Classification > RDR Settings .
The RDR Settings dialog box appears.

Step 2 Click the Transaction Usage RDRs tab.

The information under the Transaction Usage RDRs tab is displayed.

Figure 171: Transaction Usage RDRs Tab



Step 3 Check one or more of the following types of Transaction Usage RDRs to be generated:

- Generic TUR
- Only IPV6 TUR
- Protocol Specific TURs (include protocol specific information)
- Extended TURs (include extended protocol specific information)

If you select Only IPV6 TUR, the Only IPV6 TUR checkbox is enabled. Check this box to generate only the IPv6 TUR.

If you check Protocol specific TURs, the ClickStream HTTP TURs only checkbox is enabled. Check this box to generate only the HTTP TUR with clickstream signature for the selected service and packages.

If you check Extended TURS, the Anonymize - Encrypt Personally Identifiable Information checkbox is enabled. Check this box to anonymize data.

Step 4 (Optional) To enable the generation of Transaction Usage RDRs for a selected package, check the check box next to the package name in the package tree.
The package expands to show all component services of the package; all services are checked.

Step 5 Enable the generation of Transaction Usage RDRs for selected services of a package.

Step 6 Expand the node of the desired package.

Step 7 Check the check box next to the service name of each service for which a Transaction Usage RDR is to be generated.

Step 8 (Optional) Limit the generation of Transaction Usage RDRs by session size.

Step 9 Check the Generate TUR only for sessions exceeding check box.
The Bytes field is enabled.

Step 10 Enter the minimum session size in bytes for which a Transaction Usage RDR should be generated for the session.

Step 11 (Optional) Enable the generation of additional, interim Transaction Usage RDRs for long flows. (Usually, a Transaction Usage RDR is generated only when a flow closes.)

Step 12 Check the Enable Interim TUR to be generated every check box.
The Minutes field is enabled.

Step 13 Enter the required time in minutes between each generation of a Transaction Usage RDR for each flow.

Step 14 Click **OK**.
The RDR Settings dialog box closes.

The new configuration for the generation of Transaction Usage RDRs is saved.

Managing Log RDRs

Log RDRs, which provide information about system events, are generated in response to specific actions or state changes.

There are two types of Log RDRs:

- Blocking RDRs—Generated each time a transaction is blocked
- Breach RDRs—Generated each time a bucket exceeds the global threshold

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

- Blocking RDRs are generated for all packages
- Breach RDRs are always generated



Note A maximum of 20 Log RDRs are generated for each second.

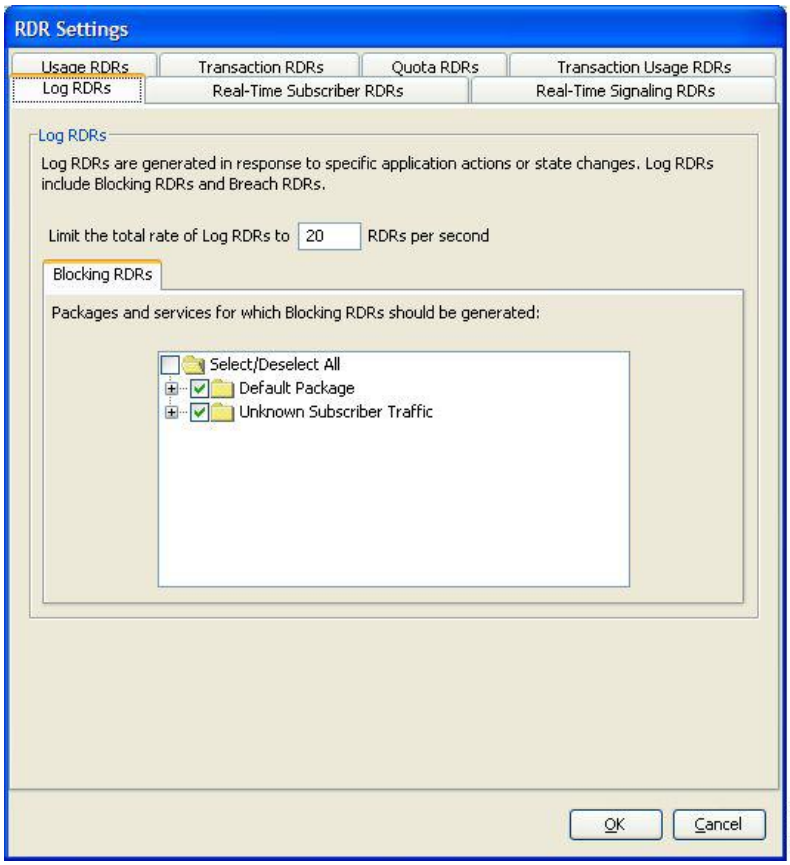
For details on the RDR purpose, default destination, content, generation logic, tag, and fields, see the Blocking RDR and Quota Breach RDR sections in the Cisco Service Control Application for Broadband Reference Guide:

Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > RDR Settings .
The RDR Settings dialog box appears.

Step 2 Click the Log RDRs tab.
The Log RDRs tab opens.

Figure 172: Log RDRs Tab



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.

Note The limit rate entered in the Log RDRs field is divided by the number of traffic processors present in the Cisco SCE. The same rate also gets updated in the respective tunable.

Step 4 To enable the generation of Blocking RDRs for selected packages, check the check box next to the package name in the package tree.
The package expands to show all component services of the package; all the services are checked.

Step 5 Enable the generation of Blocking RDRs for selected services of a package.

a) Expand the node of the desired package.
b) Check the check box next to the service name of each desired service.

Step 6 Click **OK**.
The RDR Settings dialog box closes.

The new configuration for the generation of Log RDRs is saved.

Managing Real-Time Subscriber Usage RDRs

Real-Time Subscriber Usage RDRs, which report subscriber usage, are generated for each individual subscriber for each service used, at specified intervals. These RDRs permit a more granular monitoring of selected subscribers when necessary.

For details on selecting the subscribers to be monitored, see Selecting Subscribers for Real-Time Usage Monitoring .

Note Generating and collecting Real-Time Subscriber Usage RDRs for many subscribers can compromise performance. Enable Real-Time Subscriber Usage RDR generation only for subscribers that must be monitored.

You can enable or disable the generation of Real-Time Subscriber Usage RDRs, set the generation interval for these RDRs, and set the maximum number generated per second.

By default, Real-Time Subscriber Usage RDRs:

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

For details on the RDR purpose, default destination, content, generation logic, tag, and fields, see the “Real-Time Subscriber Usage RDR” section in the Cisco Service Control Application for Broadband Reference Guide.

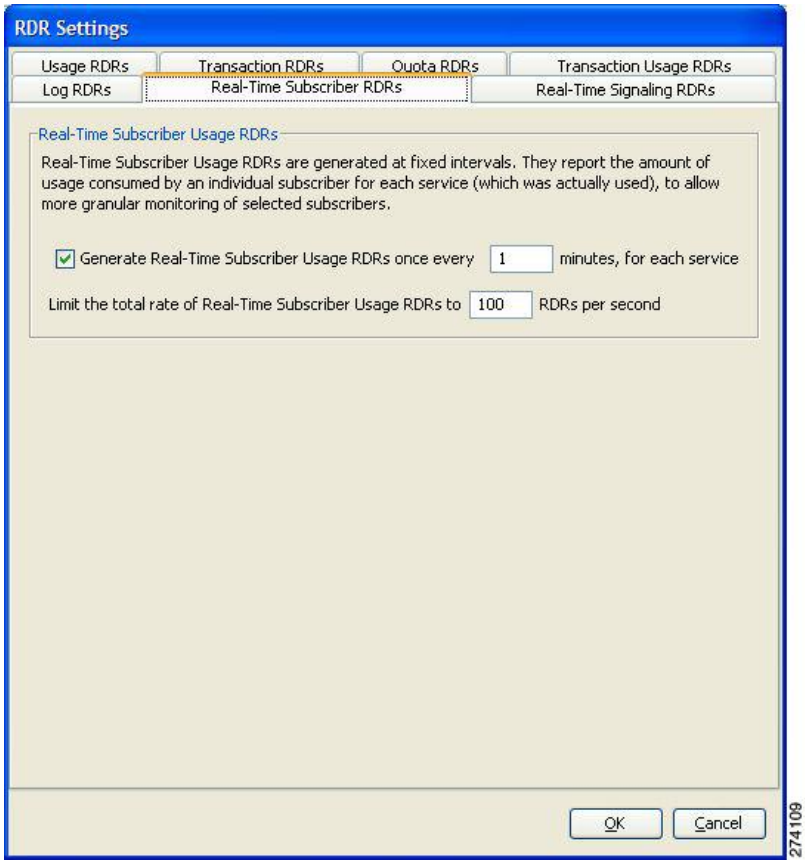
Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > RDR Settings .
The RDR Settings dialog box appears.

Step 2 Click the Real-Time Subscriber RDRs tab.

The Real-Time Subscriber RDRs tab opens.

Figure 173: Real-Time Subscriber RDRs tab



Step 3 To enable the generation of Real-Time Subscriber Usage RDRs, check the Generate Real-Time Subscriber Usage RDRs check box.

Step 4 To change the generation interval for Real-Time Subscriber Usage RDRs, enter the desired interval in minutes between each generation of the RDRs in the Generate Real-Time Subscriber Usage RDRs field.

Step 5 To limit the generation rate of Real-Time Subscriber Usage RDRs, enter the maximum number of Real-Time Subscriber Usage RDRs to be generated per second in the Limit the total rate of Real-Time Subscriber Usage RDRs field.

Step 6 Click **OK**.
The RDR Settings dialog box closes.

The new configuration for the generation of Real-Time Subscriber Usage RDRs is saved.

Managing Real-Time Signaling RDRs

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

Real-Time Signaling RDRs, are generated at the beginning and end of a flow, at specified intervals after the beginning of the flow, and at the beginning and end of a network attack.

There are two groups of Real-Time Signaling RDRs:

- Flow Signaling RDRs:
  - Flow Start Signaling RDRs
  - Flow Stop Signaling RDRs
  - Flow Interim Signaling RDRs
- Attack Signaling RDRs:
  - Attack Start Signaling RDRs
  - Attack Stop Signaling RDRs

You can enable or disable the generation of Flow Signaling RDRs for selected packages, or for selected services per package. You can set the generation interval for Flow Interim Signaling RDRs, which can be generated only if Flow Start and Flow Stop Signaling RDRs are enabled.

You can enable or disable the generation of Attack Signaling RDRs for selected packages.



Note Malicious Traffic Periodic RDRs are enabled and configured in Editing Advanced Service Configuration Options , on page 443.

For detailed information regarding the RDR purpose, default destination, content, generation logic, tag, and fields, see the following sections in the Cisco Service Control Application for Broadband Reference Guide :

- Flow Start RDR
- Flow End RDR
- Ongoing Flow RDR
- Attack Start RDR
- Attack End RDR

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

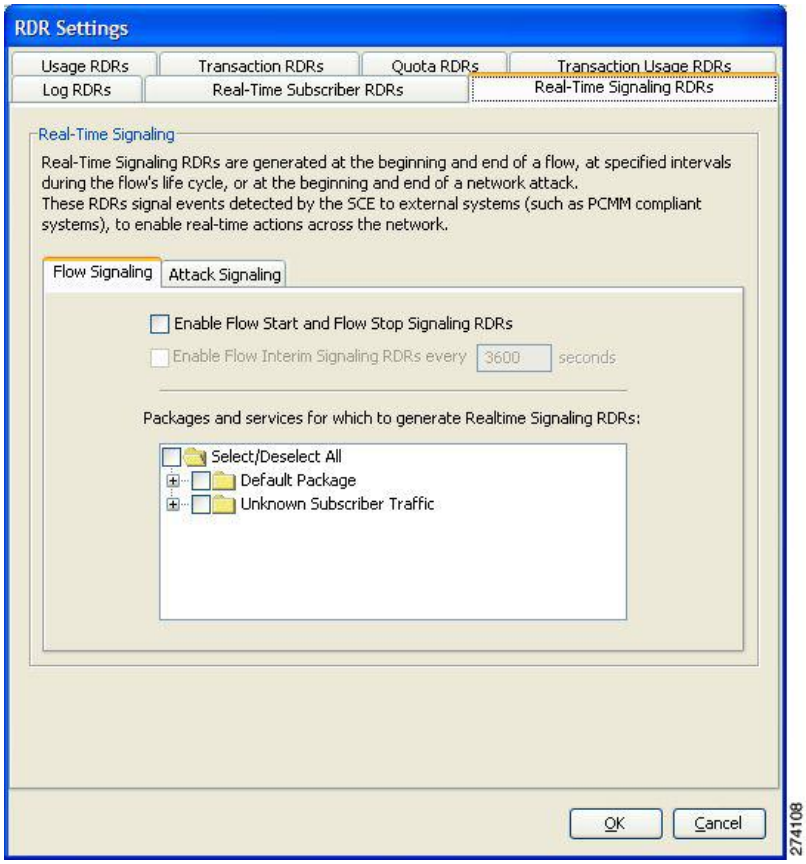
Procedure

Step 1 From the Classification tab in the left pane, choose Configuration > Classification > RDR Settings . The RDR Settings dialog box appears.

Step 2 Click the Real-Time Signaling RDRs tab.

The Real-Time Signaling RDRs tab opens.

Figure 174: Real-Time Signaling RDRs Tab



Step 3 To enable the generation of Flow Start and Flow Stop Signaling RDRs, check the Enable Flow Start and Flow Stop Signaling RDRs check box.

Note Generation of Flow Start and Flow Stop Signaling RDRs is not supported when unidirectional classification is enabled. If you try to check the Enable Flow Start and Flow Stop Signaling RDRs check box when unidirectional classification is enabled, an RDR Settings Error message appears. Click OK , and continue at Step 8.

The Enable Flow Interim Signaling RDRs check box is enabled.

Step 4 To enable the generation of Flow Interim Signaling RDRs, check the Enable Flow Interim Signaling RDRs check box.

The Enable Flow Interim Signaling RDRs field is enabled.

Step 5 To change the generation interval for Flow Interim Signaling RDRs, enter the interval in minutes between each generation of the RDRs in the Enable Flow Interim Signaling RDRs field.

Step 6 To enable the generation of Flow Interim Signaling RDRs for selected packages, check the check box next to the package name in the package tree.

The package expands to show all component services of the package; all the services are checked.

Step 7 To enable the generation of Flow Interim Signaling RDRs for selected services of a package:

a) Expand the node of the desired package.

b) Check the check box next to the service name of each desired service.

Step 8 To enable the generation of Attack Signaling RDRs:

a) In the body of the Real-Time Signaling RDRs tab, click the Attack Signaling tab.

Figure 175: Attack Signaling Tab

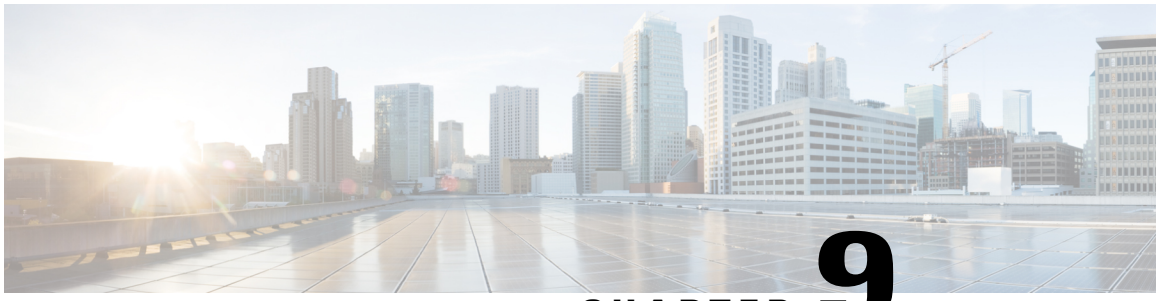


b) Check the Enable Attack Start and Attack Stop Signaling RDRs check box.

Step 9 To enable the generation of Attack Signaling RDRs for selected packages, check the check box next to the package name in the package list.

Step 10 Click OK .
The RDR Settings dialog box closes.

The new configuration for the generation of Real-Time Signaling RDRs is saved.



CHAPTER 9

Traffic Control Using the Service Configuration Editor

The Traffic Control capabilities of the Service Control Engine (Service Control platform, and the Cisco Service Control Application for Broadband) are used to limit and prioritize traffic flows. Control of traffic is based on parameters such as the service of the flow, the package of the subscriber, and the quota state of the subscriber. This chapter consists of these sections:

- Introduction to Managing Bandwidth, page 269
- Introduction to Managing Virtual Links, page 305
- Introduction to Managing Packages, page 318
- Introduction to Add-on Packages, page 326
- Introduction to Managing Rules, page 331
- Quota Management, page 360
- Unknown Subscriber Traffic , page 377

Introduction to Managing Bandwidth

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

The number of global controllers a service configuration can contain varies based on the Cisco SCE hardware. The maximum number of global controllers including the default global controllers are:

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

Note In release 3.7.5, the global bandwidth controller for IPv6 works in the subscriberless mode. The IPv6 traffic is mapped to a default subscriber (N/A). Bandwidth control should be performed on the Unknown Subscriber Package. The maximum and the default package ID of the Unknown Subscriber value is 4999.

Note If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration. A subscriber BWC that pointed to a user-defined global controller now points to the default global controller. (Other parameters of these subscriber BWCs remain unchanged.)

Managing Global Bandwidth Overview

The upstream and downstream interfaces are each assigned one default global controller that, by default, controls the total link traffic. Based on the Cisco SCE hardware, the number of global controllers you can add to a service configuration varies. For details, see the Introduction to Managing Bandwidth, on page 269 section.

You can also define the bandwidth total link limit to be less than the physical capacity of the Cisco SCE platform for each interface separately. When another device that has limited BW capacity is next to the Cisco SCE platform on the IP stream, you can have this limitation enforced in a policy-aware manner by the Cisco SCE platform, instead of having it enforced arbitrarily by the other device.

Viewing Global Controller Settings

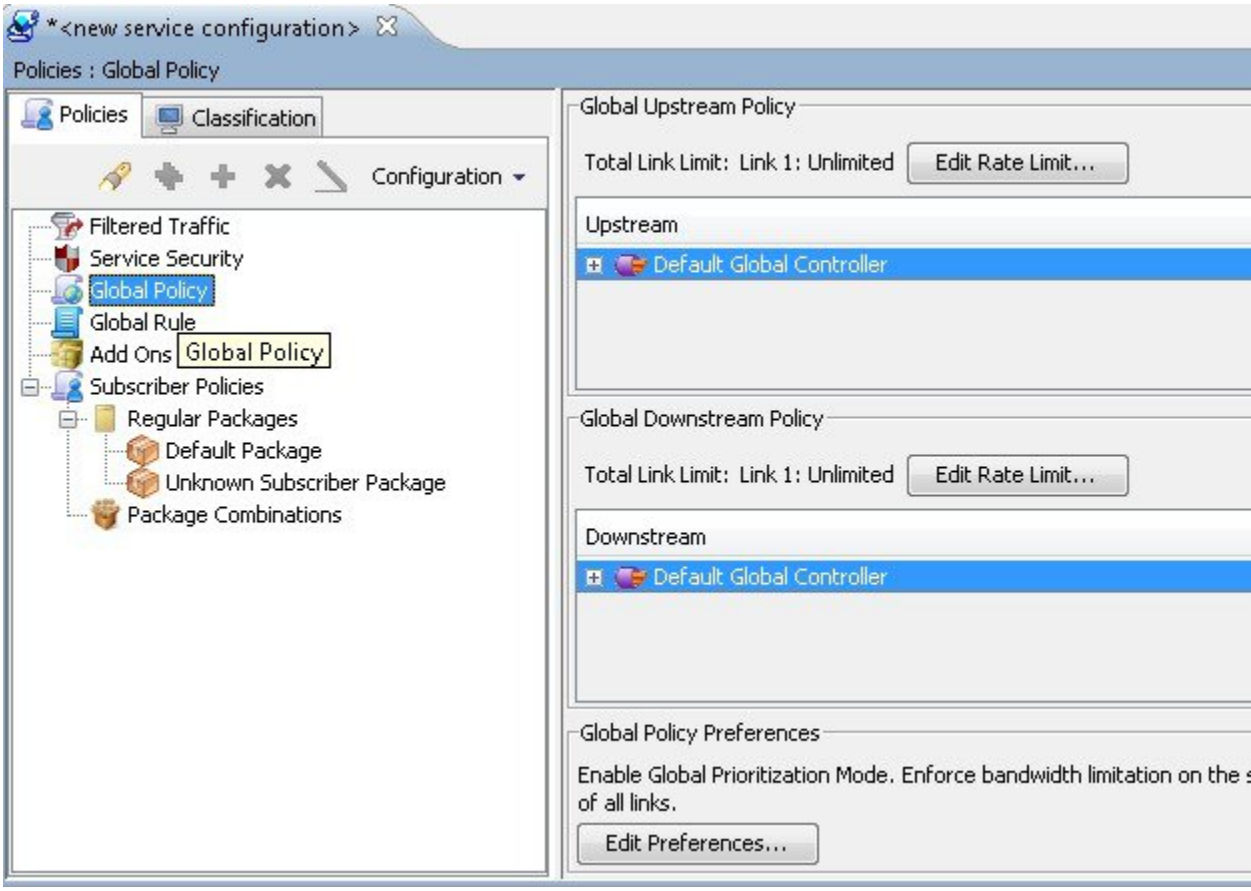
Note Global controller bandwidth is based on Layer 1 volume. Accounting, reporting, and subscriber bandwidth control in Cisco SCA BB is based on Layer 3 volume.

Procedure

In the Policies tab, click Global Policy .

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Figure 176: Global Bandwidth Settings



The two check boxes near the top of the Global Controllers tab are used only in dual-link systems (see Introduction to Defining Global Controllers, on page 274 section).

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

- Upstream or Downstream —Displays the hierarchy of global controllers, bandwidth controllers, and service rules. Each global controller has the bandwidth controllers that are connected to it listed as children. Each bandwidth controller has the service rules associated with it listed as children.
- Policy Description—Summarizes the details of the global controller, bandwidth controller, or service rule in the corresponding column. In the rows containing the global controller details, the maximum bandwidth value permitted to this global controller is displayed.

For each global controller, you can set different values for the maximum bandwidth for each of the four time frames defined by the default calendar. For details, see Managing Calendars Overview , on page 353 section.

- A single value in this field indicates that the maximum bandwidth for this global controller is constant.

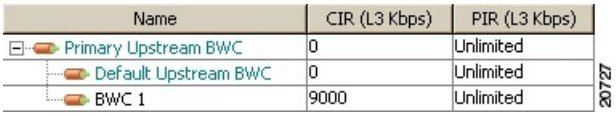
- If each time frame has a different maximum bandwidth, the maximum bandwidth for each time frame is displayed, separated by commas.

Figure 177: Time Frame Display



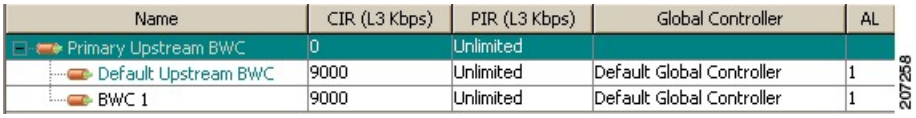
- If two time frames have the same maximum bandwidth, the value is not repeated. (So 40,,,100 means that the first three time frames have a maximum bandwidth of 40 percent of the total link limit, and the fourth time frame has a maximum bandwidth equal to the total link limit.)

Figure 178: Time Frame Details



Above the area (Upstream or Downstream) of each interface, the total link limit is displayed.

Figure 179: Total Link Time



Filtering Global Controllers

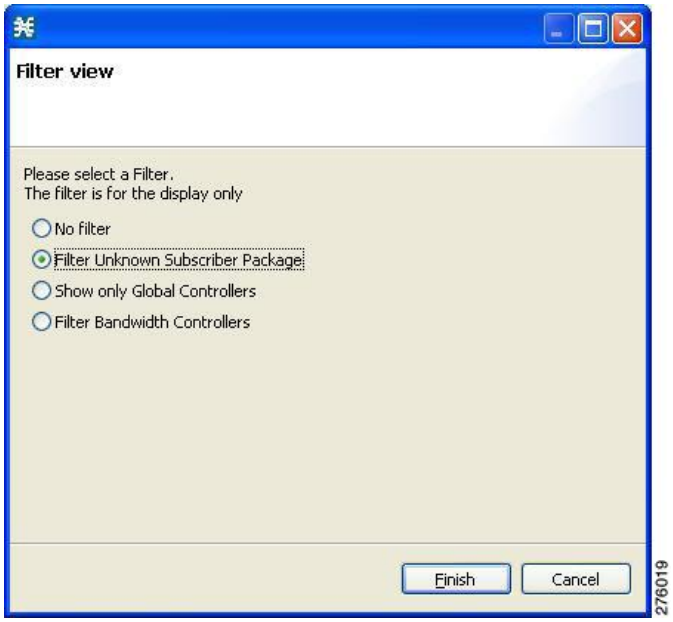
Procedure

Step 1 In the Policies tab, click Global Policy .
The Global Bandwidth Settings are displayed in the right (Rule) pane.

Step 2 Click Configure Filters.

The Filter View dialog box appears.

Figure 180: Filter View



Step 3 Choose one of the filter radio buttons:

- No Filter
- Filter Unknown Subscriber Package
- Show only Global Controllers
- Filter Bandwidth Controllers

Step 4 Click Finish.
The Filter View dialog box closes and the right (Rule) pane is filtered according to your selection.

Editing the Total Link Limits

You can limit the total bandwidth for each Cisco SCE link passing through the Cisco SCE platform.

For example, if a device connected to the Cisco SCE platform on the IP stream has limited BW capacity, you can limit the bandwidth for each Cisco SCE link passing through the Cisco SCE platform to match the capacity of the other device.

Note The total bandwidth here means the limit for each Cisco SCE link and not the aggregated limit on all the links.

The total link limits, for each Cisco SCE link, for upstream and downstream traffic are defined independently.

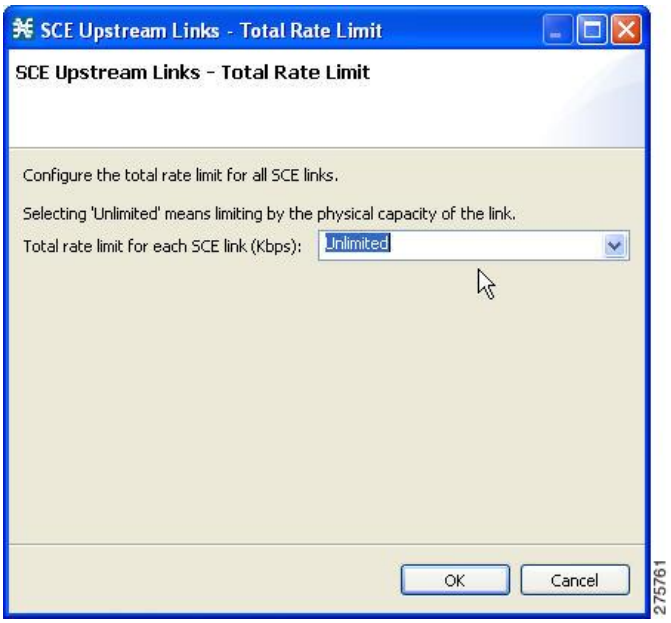
Procedure

Step 1 In the Policies tab, click **Global Policy**.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 2 In the Upstream or Downstream section, click **Edit Rate Limit**.

Note The display appearance depends on the global controller mode setting.

Figure 181: SCE Upstream Links - Total Rate Limit



Step 3 Select the total rate limit in the Total rate limit for each Cisco SCE link (Kbps) field.

Step 4 Click **OK**.
Your changes are saved.

The Global Controller Settings dialog box closes.

Introduction to Defining Global Controllers

This section describes how to define global controllers in both dual-link and multi-gigabit Ethernet systems.

In both systems, you can define each link separately with equal rates or you can define each link separately with different rates.

Alternatively, you can apply bandwidth limitations as an aggregate for all links or as an aggregate with individual control of each links.

You can:

1. Control each link separately with equal rate to all links.
2. Control each link separately without with different rate per link.
3. Control the links in aggregate and in addition maximum rate per-link, which is equal between all links.
4. Control the links in aggregate and in addition maximum rate per-link, which is different between the links.
5. Control the links in Virtual Link mode.



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



Note Any attempt to change the global controller bandwidth for invalid link results in an error message during apply policy, similar to the following: “Invalid value set on Link ID 6 for upstream GC ‘Default Global Controller’. Link ID 6 does not exist. Available Link IDs: 1, 2, 3, 4”

To activate the respective edit dialog of the Global Controller settings:

- Double click on a global controller row in the global controller table view on the right main panel of the Global Policy setting.
- Click on the edit button that is located on the top right main panel of the Global Policy setting.



Note The behavior is the same whether you configure upstream or downstream GC.

Refer to the following sections for configuration details:

Setting Global Controller Bandwidth Limits Separately with a Different Rate Per Link

Use the following procedure to configure the global controller with a different rate per link.

Procedure

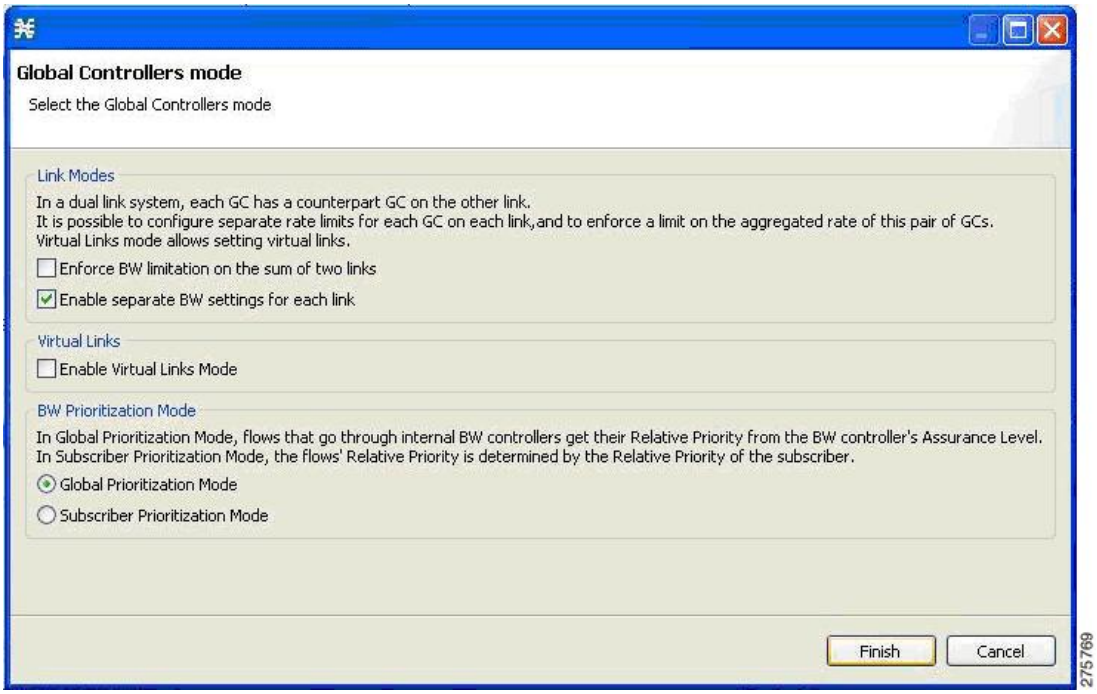
Step 1 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in Adding Global Controllers, on page 310.

Step 3 Click Edit Preferences.

The Global Controllers mode dialog box appears.

Figure 182: Global Controller Mode



Step 4 Check the Enable separate BW setting for each link check box.

Step 5 Click Finish .
The Global Controllers mode dialog box closes.

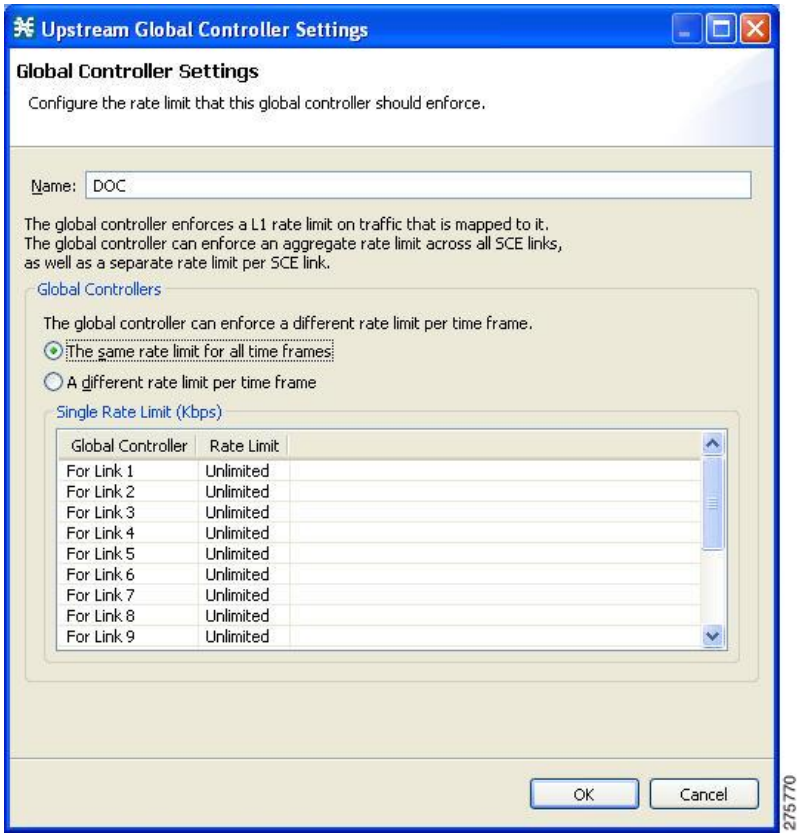
Step 6 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click the Edit ( ) icon.

The Global Controller Settings dialog box appears.

Figure 183: Downstream Global Controller Settings



Note If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries for each link.

Step 10 Choose the The same rate limit for all time frames radio button.

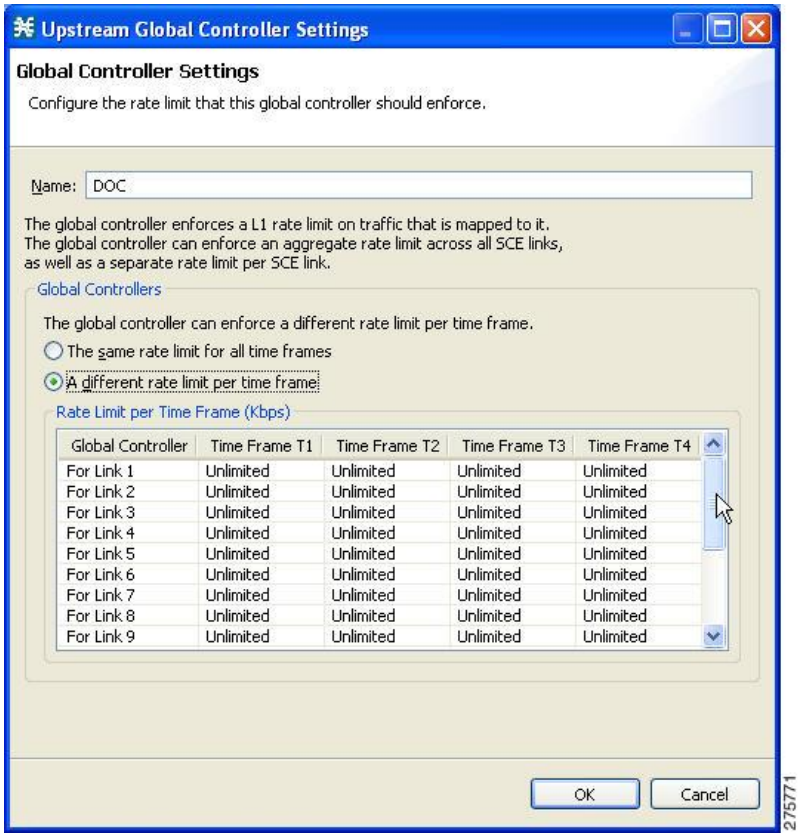
Step 11 Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

Step 12 Set the maximum limit that this global controller carries to vary according to time frame for each link.

Step 13 Choose the A different rate limit per time frame radio button.

Step 14 Enter the desired value for each time frame.

Figure 184: Upstream Global Controller Settings



Step 15 Click OK .
Your changes are saved.

Setting Global Controller Bandwidth Limits as the Sum of All Links with a Different Rate Per Link

In this link control mode, the maximum bandwidth is the sum of links but bandwidth settings can be configured for each link up the maximum bandwidth for all links. When you create a GC in this mode you can configure the aggregate global controller of the link and in addition specify a bandwidth limitation per link. This mode is used when the Cisco SCE serves multiple edge devices and you want to enforce two rules: One aggregate rule on all the links together and one rule per specific link. In this mode, you can enforce bandwidth limitation on the sum of all links and enable separate bandwidth settings for each link. You can control the links in aggregate and set maximum rate per-link which is different between the links.

Use the following procedure to configure global controller as the sum of all links with a different rate per link.

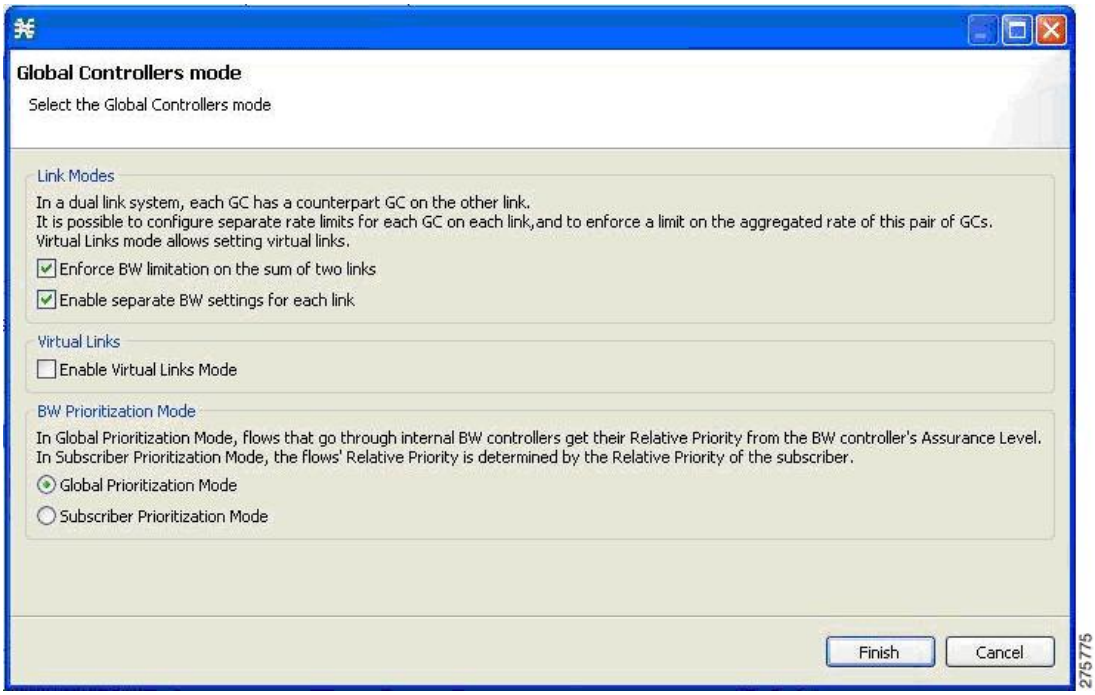
Procedure

Step 1 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in Adding Global Controllers, on page 310.

Step 3 Click Edit Preferences .
The Global Controllers mode dialog box appears.

Figure 185: Global Controllers Mode



Step 4 Check the Enforce BW limitation on the sum of the links and Enable separate BW setting for each link check boxes.

Step 5 Click Finish.
The Global Controllers mode dialog box closes.

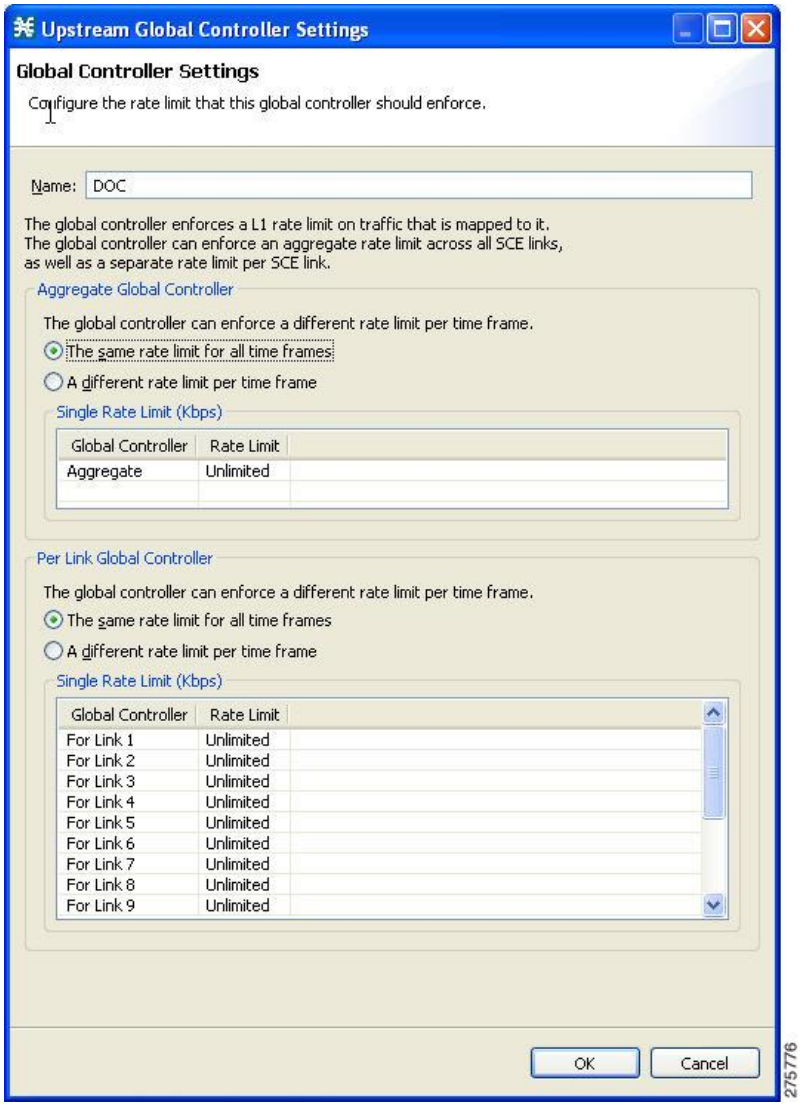
Step 6 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click the Edit ( ) icon.

The Global Controller Settings dialog box appears.

Figure 186: Upstream Global Controller Settings



Note If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries.

Step 10 Choose the same rate limit for all time frames radio button on the Per Link Global Controller tab.

Step 11 Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.

Step 12 Repeat Step 9b for each link.

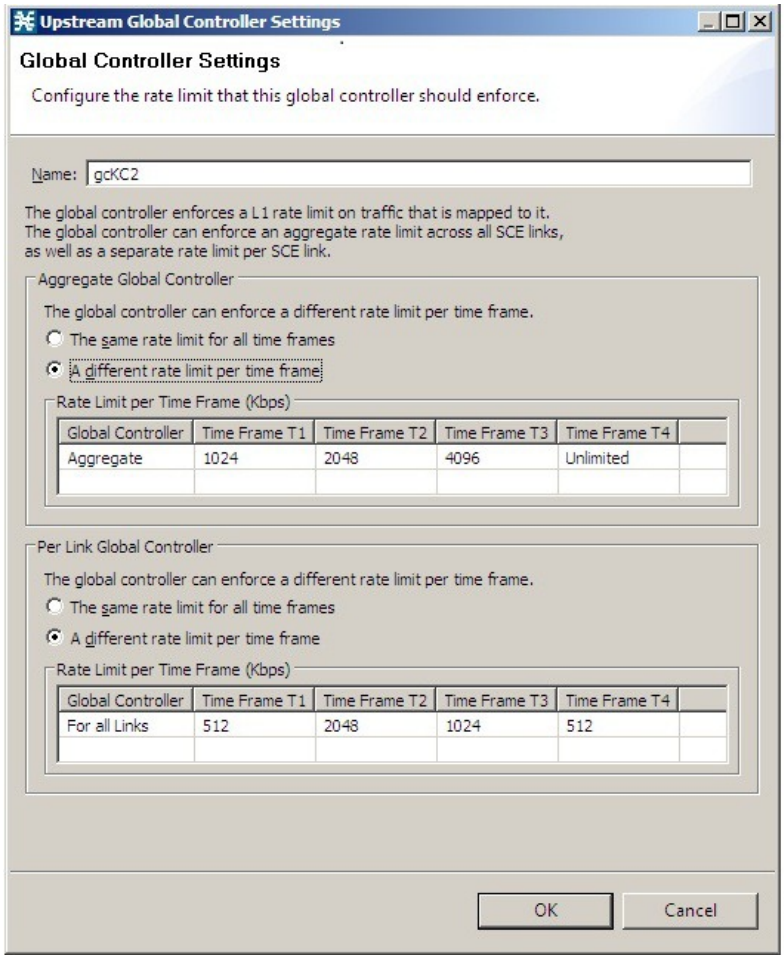
Step 13 Set the maximum limit that this global controller carries to vary according to time frame.

Step 14 Choose the A different rate limit per time frame radio button the Per Link Global Controller tab.

Step 15 Enter the desired value for each time frame.

Step 16 Repeat Step 10b for each link.

Figure 187: Downstream Global Controller Settings



Step 17 Click OK.
Your changes are saved.

Setting Global Controller Bandwidth Limits as the Sum of All Links with an Equal Rate Per Link

In this link control mode, the maximum bandwidth limitation is configured as sum of all links. When you create a GC in this mode, you can configure the aggregate global controller of the link and configure the maximum rate per link. In this mode, you can enforce bandwidth limitation on the sum of all links and control the links in aggregate and in addition maximum per-link which is equal between all links.

Use the following procedure to configure global controller as the sum of all links with an equal rate per link.

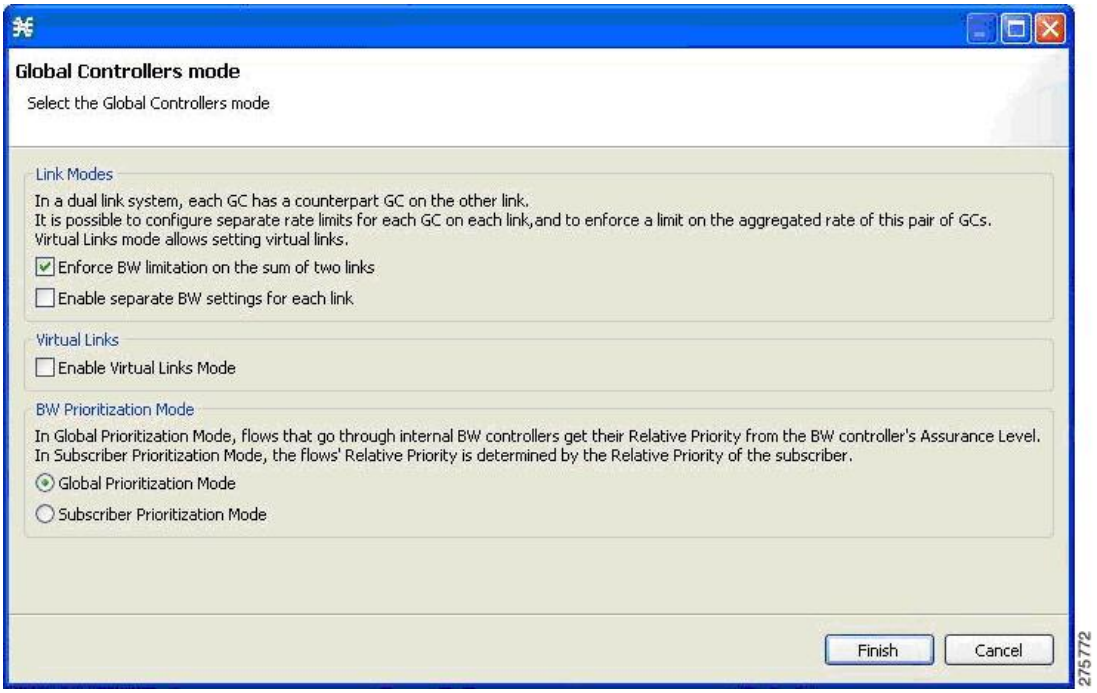
Procedure

Step 1 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in Adding Global Controllers, on page 310.

Step 3 Click Edit Preferences .
The Global Controllers mode dialog box appears.

Figure 188: Global Controllers Mode



Step 4 Check the Enforce BW limitation on the sum of the links check box.

Step 5 Click Finish .
The Global Controllers mode dialog box closes.

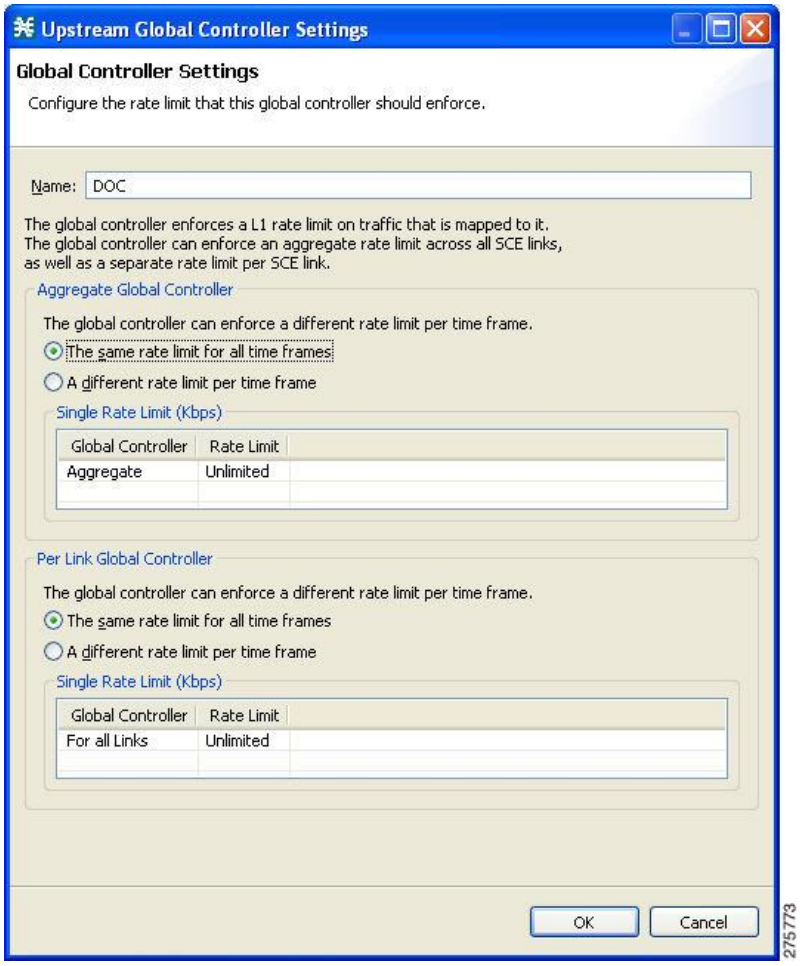
Step 6 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click the Edit ( ) icon.

The Global Controller Settings dialog box appears.

Figure 189: Upstream Global Controller Settings



Note If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries.

Step 10 Choose the **The same rate limit for all time frames** radio button on the Aggregate Global Controller tab.

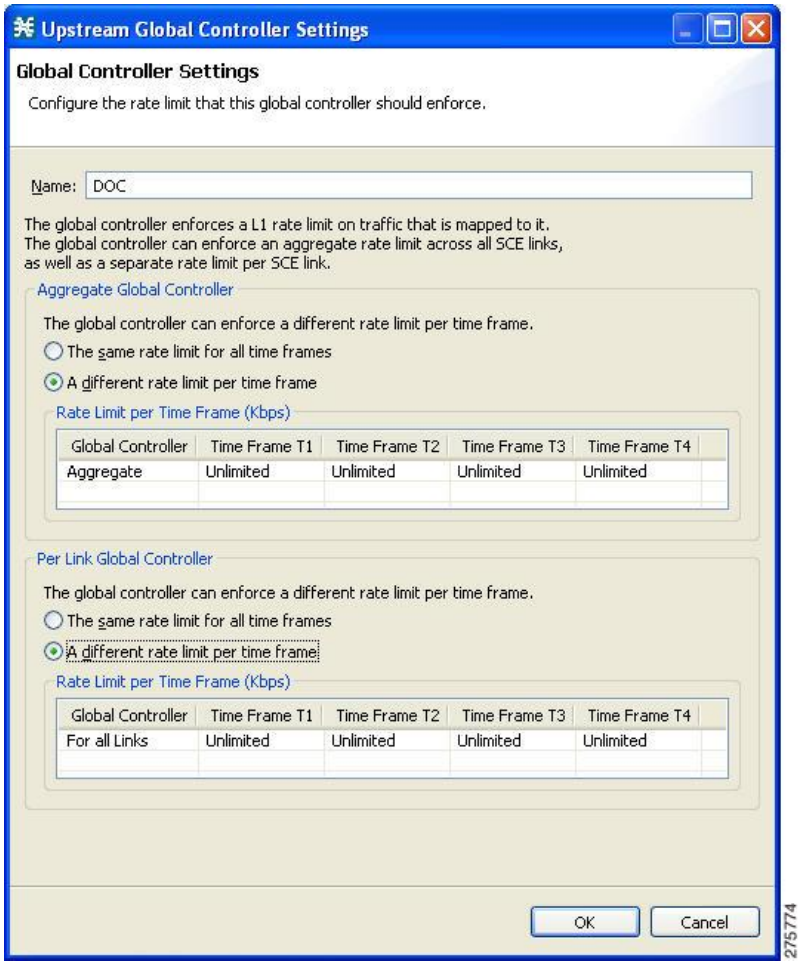
Step 11 Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

Step 12 Set the maximum limit that this global controller carries to vary according to time frame.

Step 13 Choose the A different rate limit per time frame radio button the Aggregate Global Controller tab.

Step 14 Enter the desired value for each time frame.

Figure 190: Upstream Global Controller Settings



Step 15 Click OK.
Your changes are saved.

Setting Global Controller Bandwidth Limits with Equal Rate for All Links

Use the following procedure to configure the global controller with equal rate for all links.

Procedure

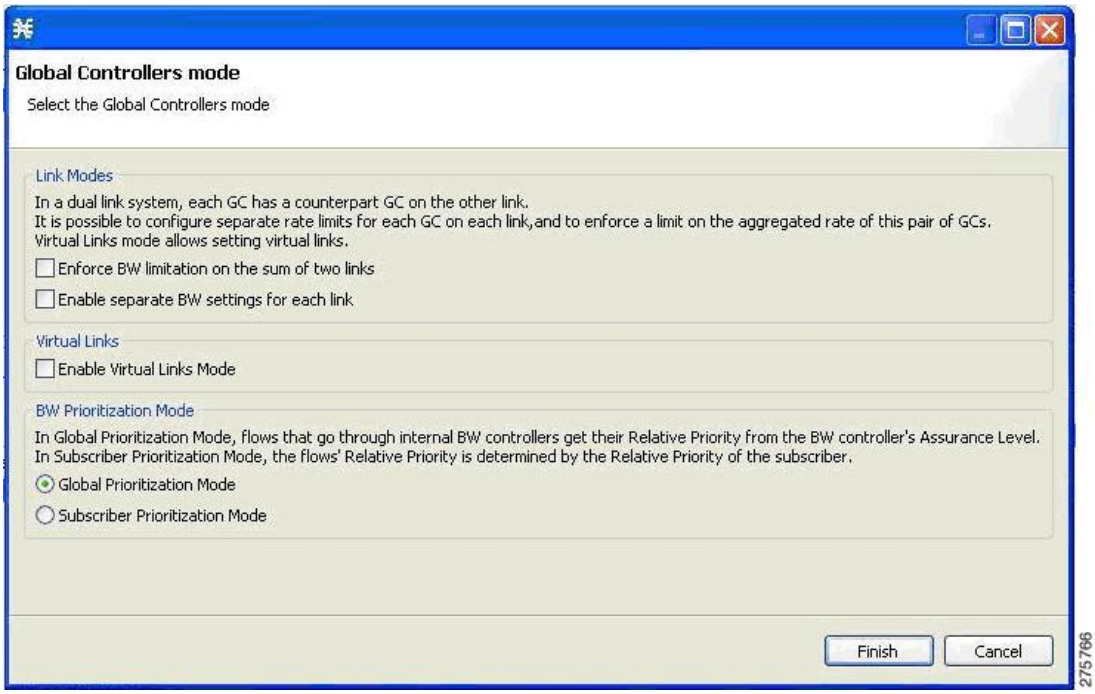
Step 1 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in Adding Global Controllers, on page 310.

Step 3 Click Edit Preferences .

The Global Controllers mode dialog box appears.

Figure 191: Global Controllers Mode



Step 4 Verify that the Link Modes check boxes are unchecked.

Step 5 Click Finish.
The Global Controllers mode dialog box closes.

Step 6 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click the Edit ( ) icon.

The Global Controller Settings dialog box appears.

Figure 192: Upstream Global Controller Settings



Note If the rate limit for all time frames is to be the same, use Step 9. If the rate limit for all time frames is to vary by time frame, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries.

Step 10 Choose the same rate limit for all time frames radio button.

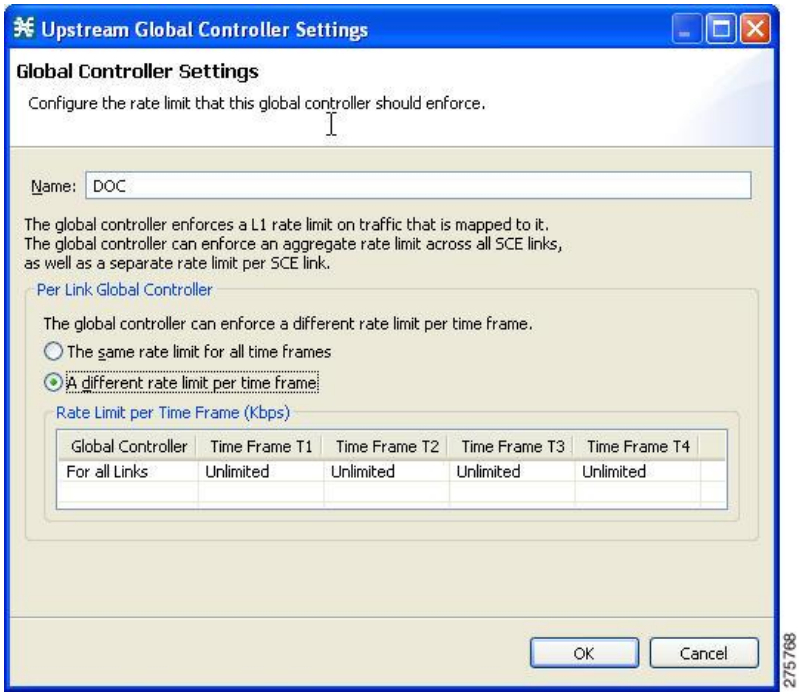
Step 11 Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Per Link Global Controller (in Kbps) field.

Step 12 Set the maximum limit that this global controller carries to vary according to time frame.

Step 13 Choose the A different rate limit per time frame radio button.

Step 14 Enter the desired value for each time frame.

Figure 193: Upstream Global Controller Settings



Step 15 Click OK .
Your changes are saved.

Setting Global Controller Bandwidth for Virtual Links

In this mode, you can control each link separately using configured rate templates and default rates. The template rate limits are applied to newly created virtual links. The default rate limits are applied to the default virtual link (virtual link 0).

Procedure

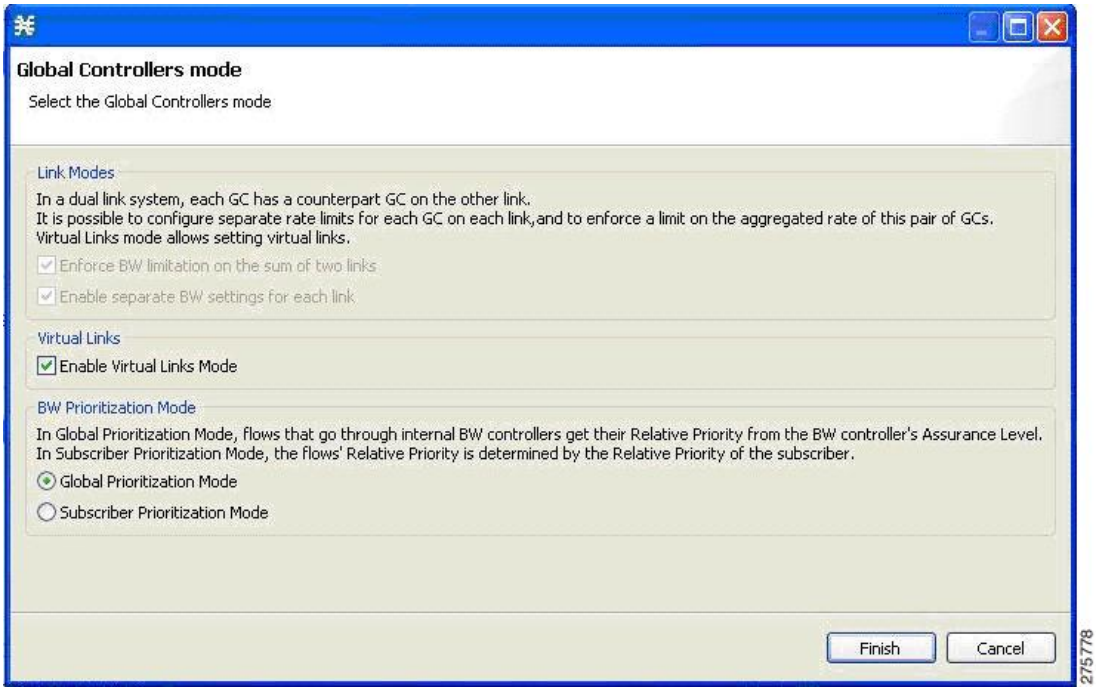
Step 1 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add global controllers, as described in Adding Global Controllers, on page 310How to Add Global Controllers, page 9-7 .

Step 3 Click Edit Preferences .

The Global Controllers mode dialog box appears.

Figure 194: Global Controllers Mode



Step 4 Check the Enable Virtual Links Mode check box.

Step 5 Click Finish.
The Global Controllers mode dialog box closes.

Note By default, the Virtual Link Mode works only in Subscriber Prioritization Mode.

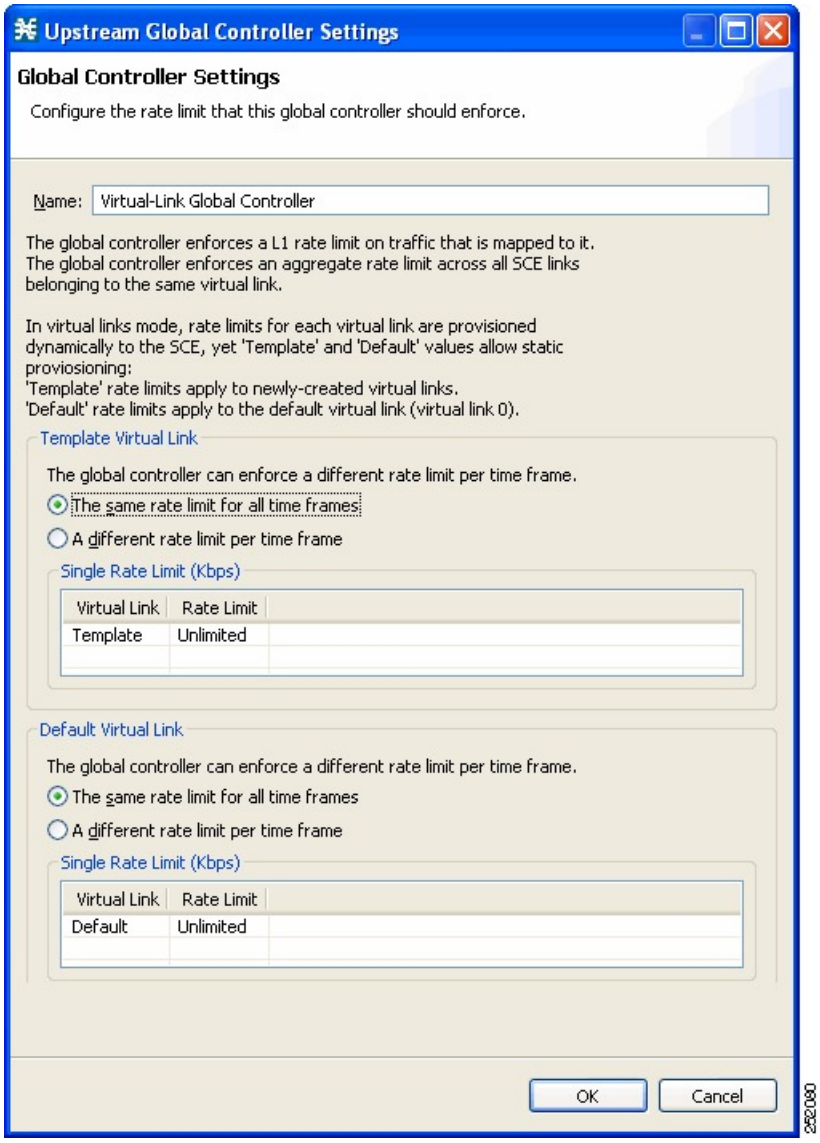
Step 6 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 7 Select a global controller.

Step 8 Click ( ) Edit.

The Global Controller Settings dialog box appears.

Figure 195: Upstream Global Controller Settings



Note If the rate limit for all time frames is to be the same for the Template Virtual Link, use Step 9. If the rate limit for all time frames is to vary by time frame for the Template Virtual Link, use Step 10.

Step 9 Set a single value for the maximum bandwidth limit that this global controller carries.

Step 10 Choose the same rate limit for all time frames radio button on the Template Virtual Link tab.

Step 11 Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.

Step 12 Set the maximum limit that this global controller carries to vary according to time frame.

Step 13 Choose the A different rate limit per time frame radio button the Template Virtual Link tab.

Step 14 Enter the desired value for each time frame.

Note If the rate limit for all time frames is to be the same for the Default Virtual Link, use Step 11. If the rate limit for all time frames is to vary by time frame for the Default Virtual Link, use Step 12.

Step 15 Set a single value for the maximum bandwidth limit that this global controller carries.

Step 16 Choose the The same rate limit for all time frames radio button on the Default Virtual Link tab.

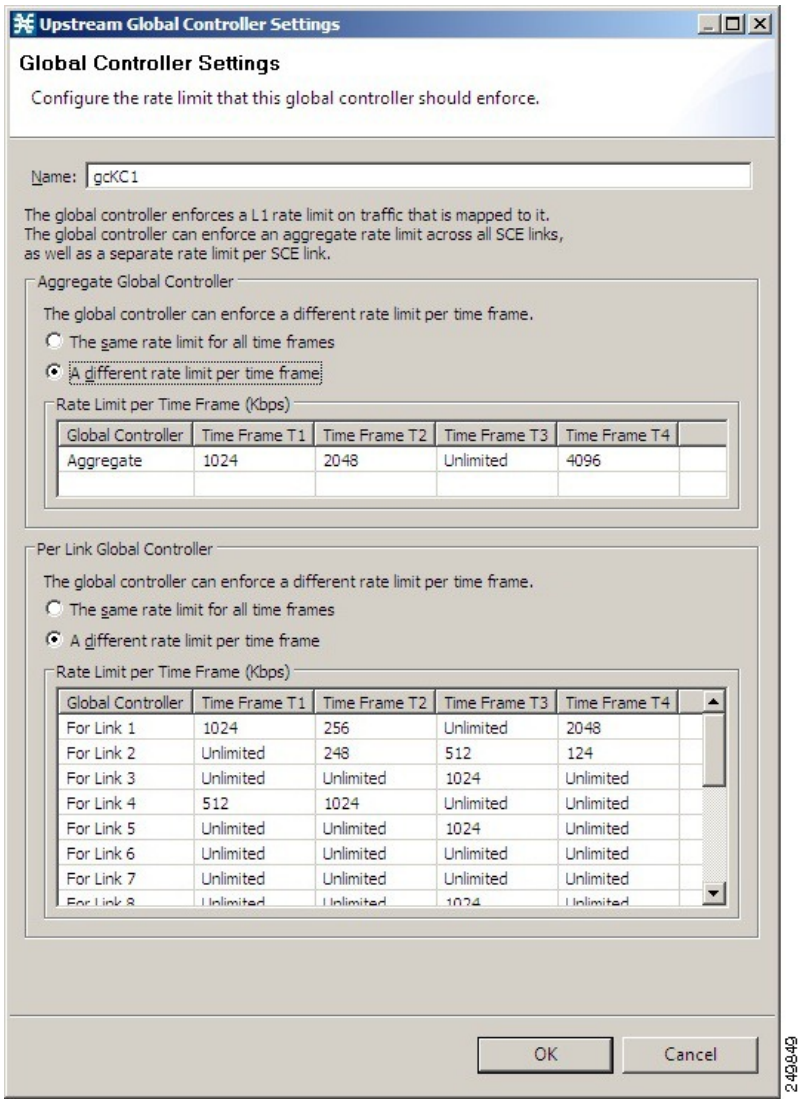
Step 17 Enter the desired value in Kbps for the maximum bandwidth in the Rate limit for the Link 1 (in Kbps) field.

Step 18 Set the maximum limit that this global controller carries to vary according to time frame.

Step 19 Choose the A different rate limit per time frame radio button the Default Virtual Link tab.

Step 20 Enter the desired value for each time frame.

Figure 196: Upstream Global Controller Settings



Step 21 Click OK.
Your changes are saved.

Introduction to Managing Subscriber Bandwidth

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

A Subscriber BWC controls subscriber bandwidth consumption for upstream or downstream flows. It controls and measures the bandwidth of an aggregation of traffic flows of a service or group of services.

Each package has its own set of BWCs that determine the bandwidth available per package subscriber for each available service.

The two Primary BWCs, one for upstream traffic and one for downstream traffic, allocate bandwidth to specific subscribers. Bandwidth is allocated based on the Committed Information Rate (CIR), the Peak Information Rate (PIR), and the Subscriber relative priority settings. You can configure these parameters, but the Primary BWCs cannot be deleted.

There are two default BWCs, one for upstream traffic and one for downstream traffic. By default, all services are mapped to one of these two BWCs. The BWC mechanism controls rate subpartitioning within the default BWC rate control, based on the CIR, PIR, and AL. You can configure these parameters, but the default BWCs cannot be deleted.

You can add up to 32 user-defined BWCs per package:

- Subscriber BWCs operate at the service-per-subscriber level. They allocate bandwidth for services for each subscriber, based upon the CIR, PIR, global controller, and Assurance Level (AL) set for the BWC. Each rule defines a link between the flow of the service and one of the BWCs (unless the flows are to be blocked). See Defining Per-Flow Actions for a Rule , on page 335 section.
- Extra BWCs also operate at the subscriber level. Extra BWCs (based on the CIR, PIR, global controller, and AL) can be allocated for services that are not included in the Primary BWC. These are services that are not often used but have strict bandwidth requirements, for example, video conference calls. The Extra BWCs are BWCs that control a single service (or service group). BWCs cannot borrow bandwidth from Extra BWCs and vice versa.

Each user-defined BWC controls either downstream or upstream traffic.



Note If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration. A BWC that pointed to a user-defined global controller now points to the default global controller. Other parameters of these BWCs remain unchanged.

The Cisco SCE supports a maximum of 2000 BWCs. You cannot apply a PQB file to a Cisco SCE if the file contains more than 2000 BWCs. But, the Subscriber BWCs with same values for GC Index, AL Level, PIR, and CIR are considered as a single BWC; even if the BWCs are mapped to different flows. So, in effect, Cisco SCA BB may support more than 2000 BWCs.

Subscriber BWC Parameters

The Subscriber BW Controllers tab of the Package Settings dialog box has the following configuration parameters:

- Name—A unique name for each BWC.
- CIR (L3 Kbps)—The minimum bandwidth that must be granted to traffic controlled by the BWC.

- PIR (L3 Kbps)—The maximum bandwidth allowed to traffic controlled by the BWC.

Note The minimum bandwidth for a subscriber BWC is 16 Kbps with a granularity of 1 Kbps and the maximum bandwidth is 1000000 Kbps.

- Global Controller—The global controller with which this BWC is associated. The global controllers are virtual queues that are part of the bandwidth control mechanism. Direct traffic with similar bandwidth control properties to the same global controller.
- Assurance Level—How fast bandwidth either decreases from the PIR to the CIR as congestion builds or else increases from the CIR to the PIR as congestion decreases. A higher AL ensures a higher bandwidth compared to a similar BWC with a lower AL. The lowest assurance value is 1, the highest is Persistent (10).
  Assurance Level 10 (persistent) never goes below the relevant CIR, unless the total line rate cannot sustain this value.
- Subscriber relative priority—Assurance Level given to the Primary BWC of the subscriber. It determines the assurance given to all the subscriber traffic when competing for bandwidth with subscribers to other packages. The lowest value is 1; the highest is 10.

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

Editing Package Subscriber BWCs

Procedure

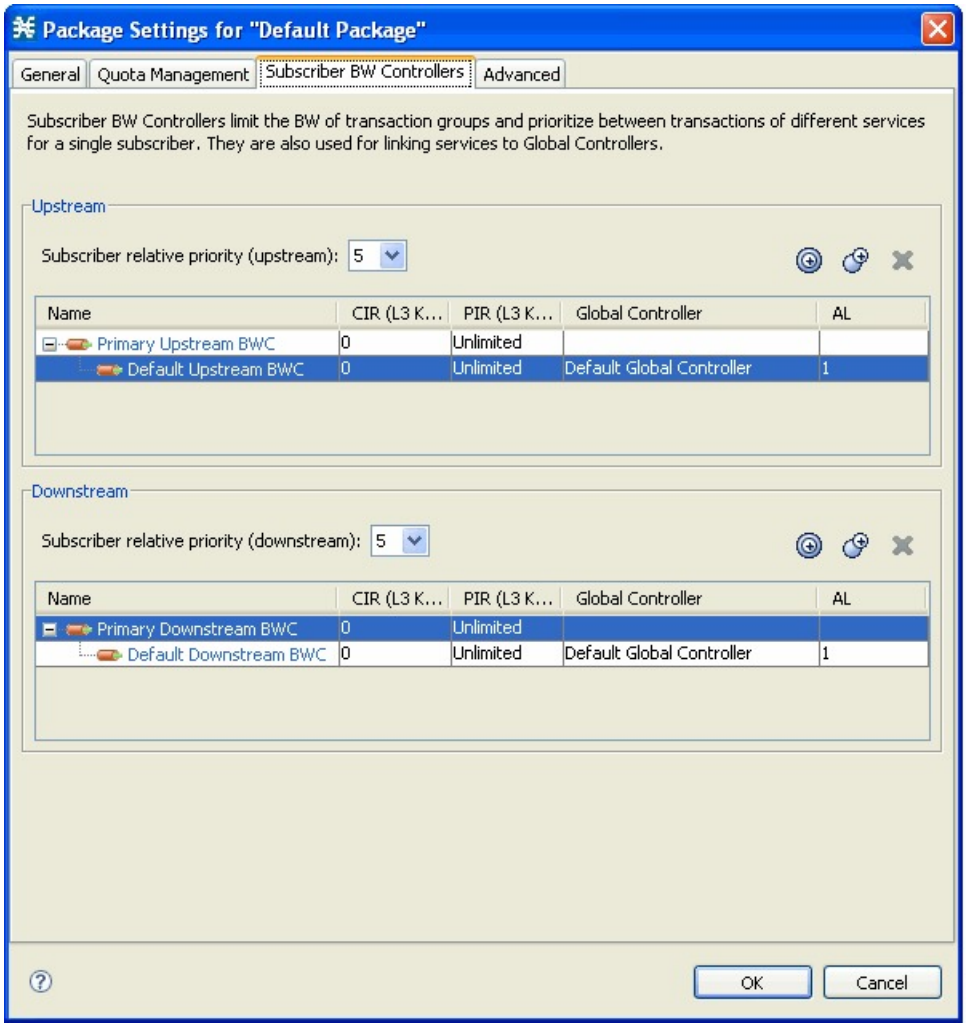
Step 1 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 In the right (Rule) pane, select a BWC and click the Edit ( ) icon.
The Package Settings dialog box appears.

Step 3 In the Package Settings dialog box, click the Subscriber BW Controllers tab.

The Subscriber BW Controllers tab opens.

Figure 197: Subscriber BW Controllers Tab



Step 4 Set your requirements for upstream bandwidth control in the Upstream area of the dialog box.

Step 5 Select a value from the Subscriber relative priority drop-down list.

Step 6 Set the parameters for the Primary Upstream BWC.

a) In the CIR field, enter the BWC CIR in Kbps.

b) In the PIR field, select Unlimited from the drop-down list, or enter the BWC PIR in Kbps.

c) To add BWCs to the package, click the Add a sub BW Controller ( ) icon once for each additional BWC.

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

Step 7 Set the parameters for each BWC (including the Primary and Default BWCs).

a) (Optional) In the Name field, enter a meaningful name for each BWC. (You cannot rename the Primary or Default BWCs.)
b) In the CIR field, enter a value for the BWC CIR in Kbps.
c) In the PIR field, select Unlimited from the drop-down list, or enter a value for the BWC PIR in Kbps.

Step 8 Set the global controller, with which this BWC is associated:

a) Click in the Global Controller cell of the BWC, and then click the Browse button that appears.
The Select a Global Controller dialog box appears.

Figure 198: Select a Global Controller



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

Step 9 Repeat Step 3 for downstream bandwidth control in the Downstream area of the dialog box.

Step 10 Click OK.
The Package Settings dialog box closes.

All changes to the BWC settings are saved.

The effect of Assurance Level on bandwidth allocation for subscriber BWCs will be as follows:

If there are 4 BWCs namely “Priority”, “Gold”, “Silver” and “default” with Assurance Levels 9, 6, 3 and 1 respectively, the “priority” BWC gets the bandwidth first, followed by the "Gold" and the "Silver" BWC. The “default” BWC will be the last to get the bandwidth.

A Practical Example of Managing Bandwidth

This section explains how to achieve effective bandwidth control by combining the configuration of global controllers and subscriber BWCs, and gives a practical example.

Configuring Total Bandwidth Control

Procedure

Step 1 Configure the necessary global controllers.
Ascertain which services are likely to be problematic, and what the maximum total bandwidth should be for each. You do not need to configure services and packages that are unlikely to be problematic; you can include them in the default global controllers.

Step 2 Configure the subscriber BWCs for the package.

Step 3 Add a subscriber BWC for each type of upstream or downstream traffic that you want to limit, and configure the CIR and the PIR accordingly.

Step 4 Select an appropriate global controller for each subscriber BWC.

Step 5 For each service that is to have its own BWC, create a rule and select appropriate upstream and downstream BWCs.

Example for Limiting P2P and Streaming Traffic Using the Console

Note This example assumes that the traffic flow is bidirectional; you may decide that you only need upstream controllers or downstream controllers.

Note The P2P Traffic Optimization wizards allow you to create a simple model of devices, connect to them, and limit P2P traffic to a specified bandwidth. (See Using the P2P Traffic Optimization Wizards , on page 81 section.)

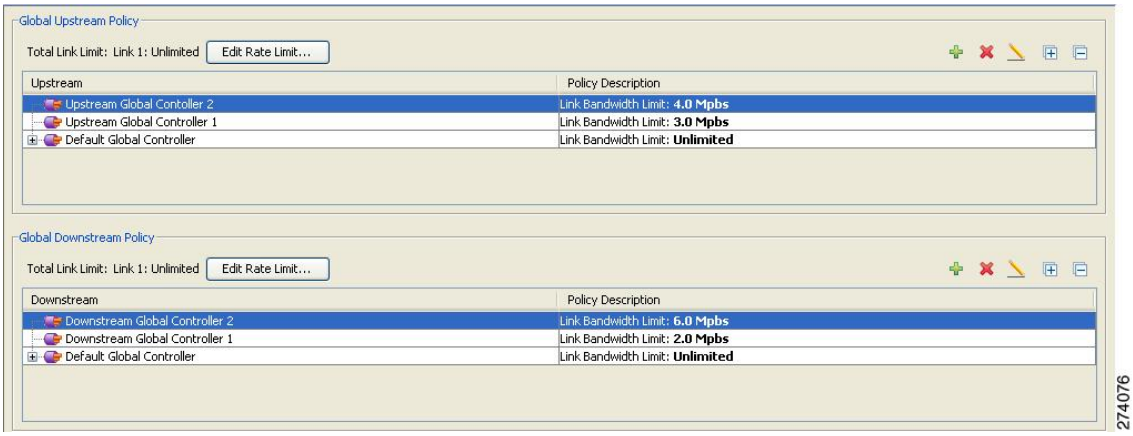
Procedure

Step 1 In the Policies tab, click Global Policy.

The Global Bandwidth Settings dialog box in the right (Rule) pane.

Step 2 Add two upstream global controllers and two downstream global controllers and assign the desired bandwidth to each global controller.

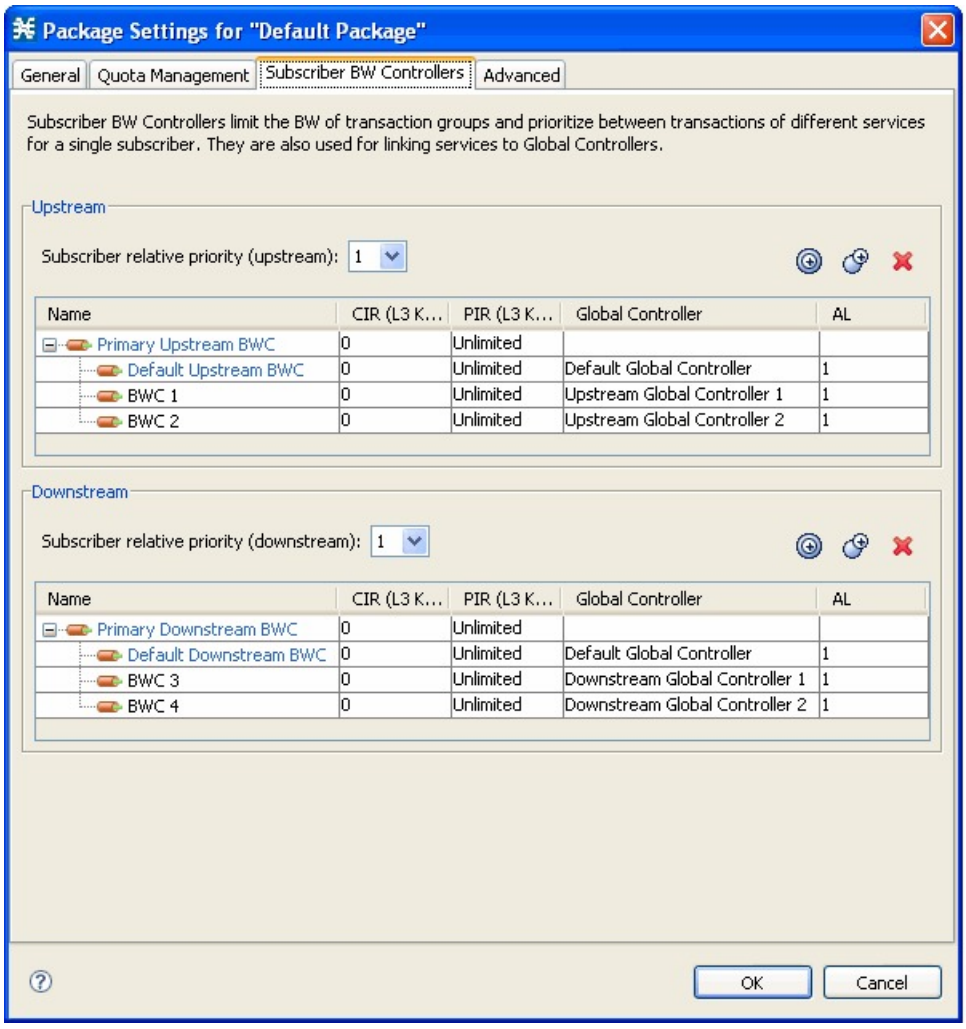
Figure 199: Global Bandwidth Settings



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

Step 3 In a Package Settings dialog box, add two upstream BWCs and two downstream BWCs, map them to the appropriate global controllers, and set their parameters (CIR, PIR, AL).

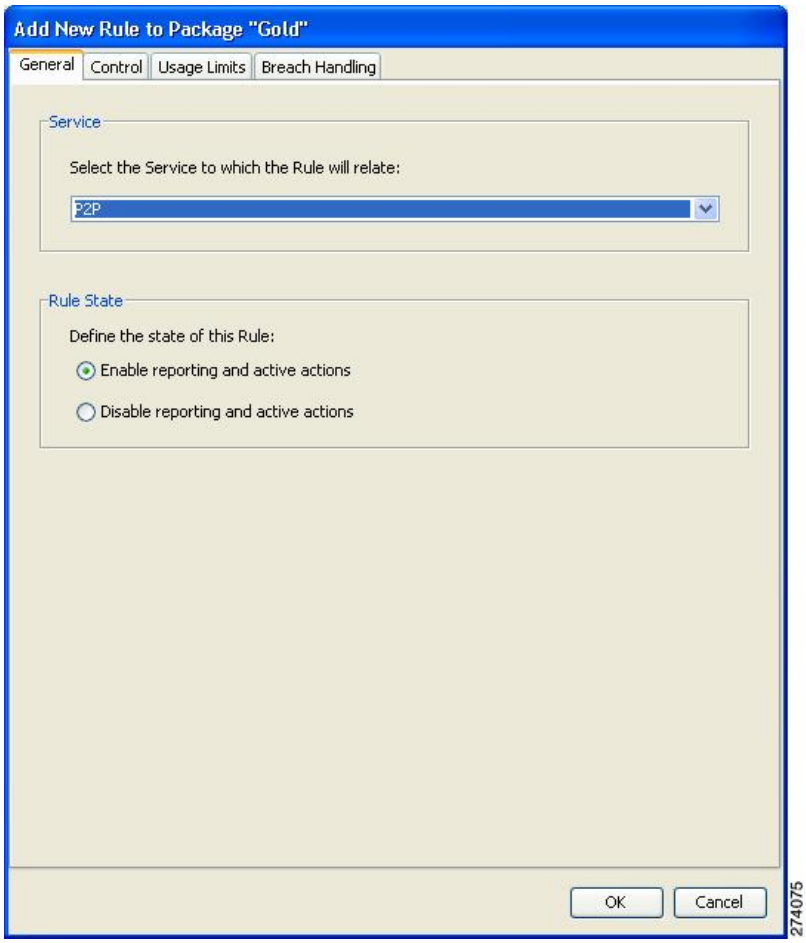
Figure 200: Package Settings



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

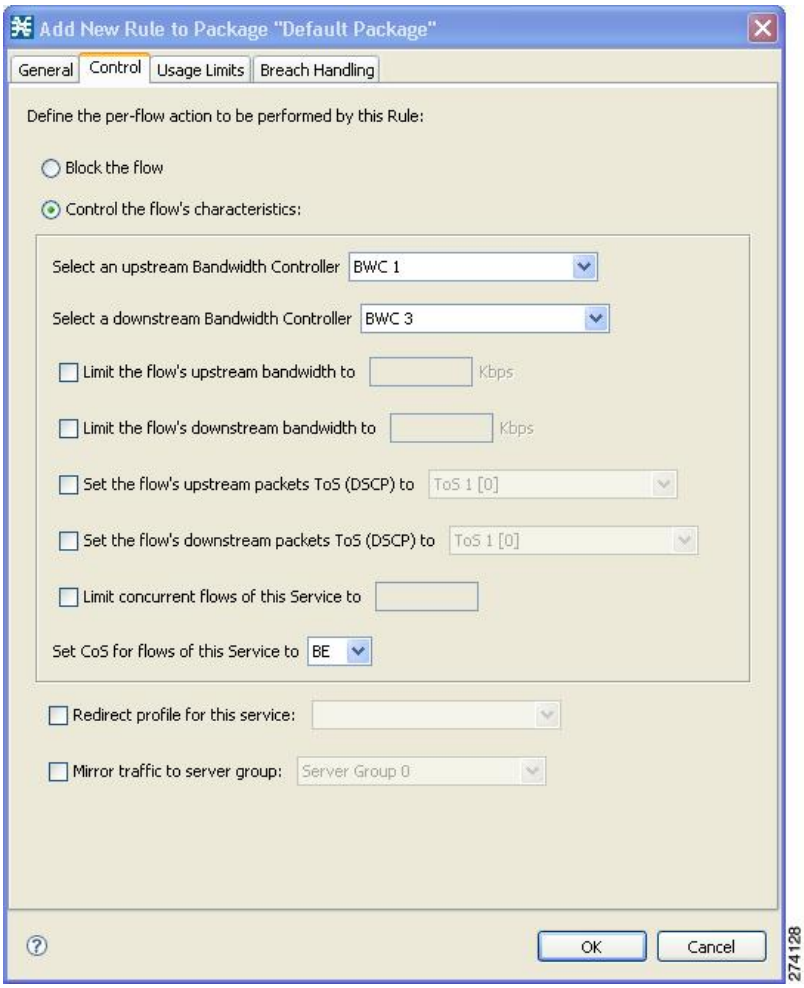
Step 4 Add a rule for the P2P service.

Figure 201: Add New Rule to Package



Step 5 In the Control tab, assign BWC 1 as the upstream BWC and BWC 3 as the downstream BWC.

Figure 202: Control Tab

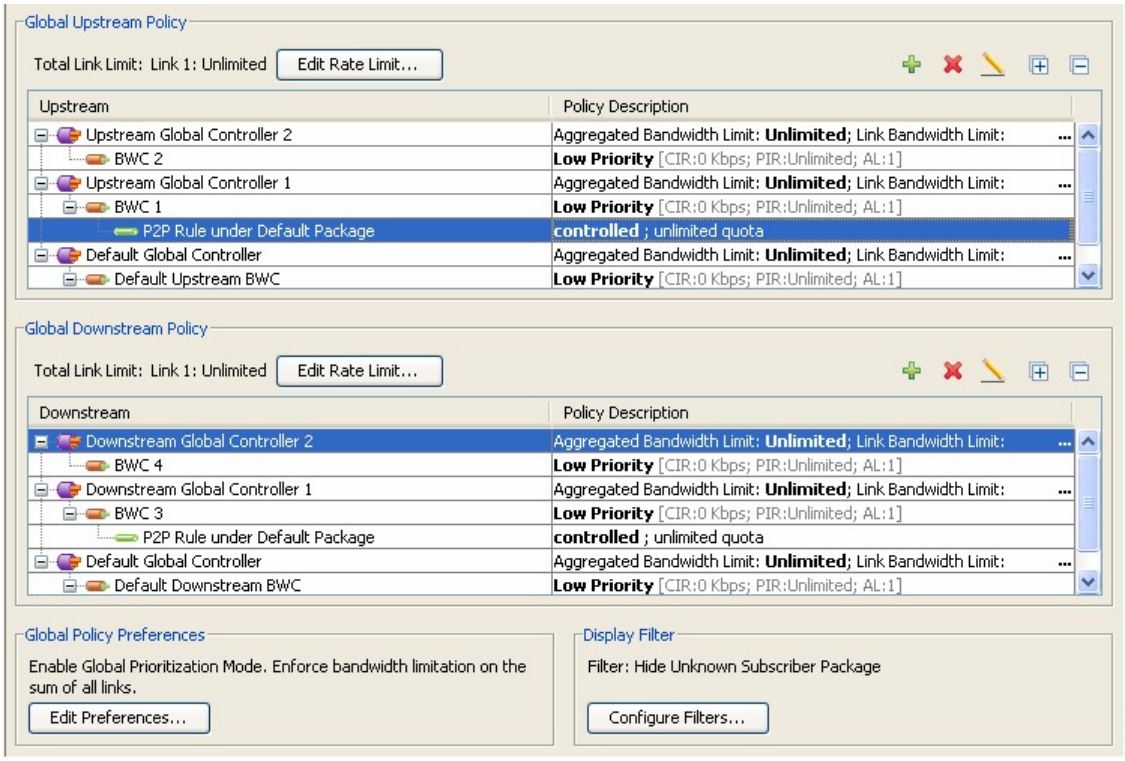


Step 6 Repeat Step 4 and Step 5 for the Streaming service, using BWC 2 as the upstream BWC and BWC 4 as the downstream BWC.

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

Step 7 Click Global Policy to view the hierarchy of the GCs, BWCs, and rules.

Figure 203: Rule Hierarchy



Configuring a Rule, Bandwidth Controller, and Global Controller Using the Wizard

You can configure a rule, BWC, and GC together from the Global Policy window.

Procedure

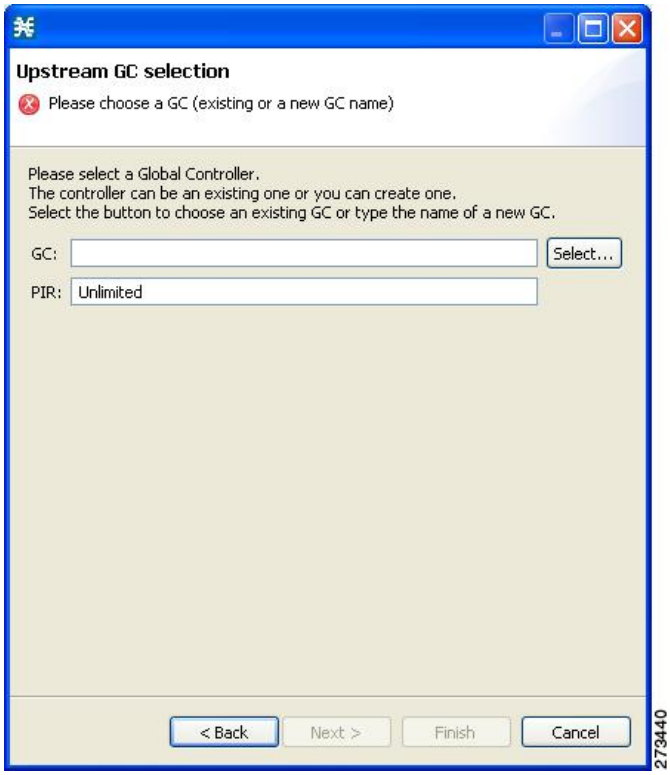
Step 1 In the Policies tab, click Global Policy .
The Global Bandwidth Settings are displayed in the right (Rule) pane.

Step 2 Above the area (Upstream or Downstream) of the desired interface, click the Add ( ) icon.
The Select addition mode dialog box appears.

Step 3 Choose the Add a Global Controller and map a Rule and BWC to it radio button.

Step 4 Click Finish.
The GC Selection dialog box appears.

Figure 204: Upstream GC Selection



Step 5 In the GC field, enter a new GC name, or click Select to choose an existing GC.

Step 6 (Optional) In the PIR field, enter the maximum bandwidth limit that this global controller carries in Kbps.

Step 7 Click Next.

The Service and Packages selection dialog box appears.

Figure 205: Upstream Service and Packages Selection



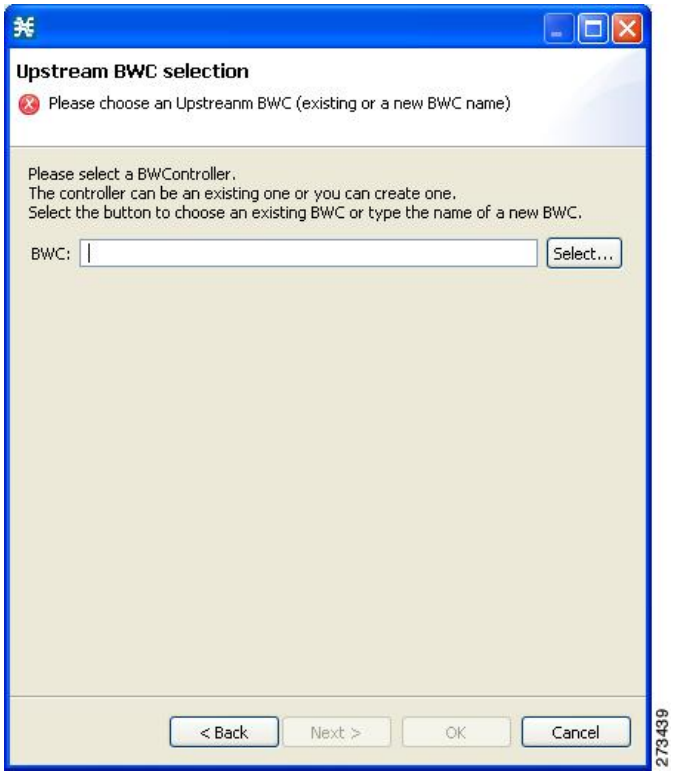
Step 8 In the Service field, select an existing service.

Step 9 In the Packages section, select one or more packages for the rule to apply to.
If a rule does not exist for the service, it is created. The new, or existing rule is then mapped to the selected package or packages.

Step 10 Click Next.

The BWC selection dialog box appears.

Figure 206: Upstream BWC Selection



Step 11 Enter a new BWC name, or click Select to choose an existing BWC.

Step 12 Click OK .

Configuring the Upstream Configuration of the Global Bandwidth Controller for IPv6

You can configure the upstream configuration of the global bandwidth controller for IPv6 from the Global Policy window. For details on managing the bandwidth, see the Introduction to Managing Bandwidth, on page 269"Managing Bandwidth" section.

Procedure

Step 1 In the Service Configuration Editor window, click the Policies tab.

Step 2 Under the Policies tab, click Global Policy.

The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 3 Above the area (Upstream or Downstream) of the corresponding interface, click the Add ( ) icon.
The Select Addition mode dialog box is displayed.

Step 4 Click the Add a Global Controller and map a Rule and a BWC to it radio button to add a global controller with a rule mapped to it and a BWC added to it.

Step 5 Select an existing global controller by clicking the Select button or create a new global controller by typing the name of a global controller.

Step 6 Enter the PIR value and click Next.

Step 7 Select the service to control and check the Unknown Subscriber Package check box and Click Next.

Step 8 Select an existing BWC by clicking the Select button or create a new BWC by typing the name of the BWC. Click Next.

Step 9 Double-click on the unknown subscriber package to verify the bandwidth controller and the global controller association.

What to Do Next

Follow the same procedure for the downstream configuration of the global bandwidth controller for IPv6.

Setting Bandwidth Management Prioritization Mode

Relative priority is the level of assurance that an internal BWC (iBWC) receives when competing against other iBWCs for bandwidth.

The relative priority of one of the following modes determines the relative priority of the flow that goes through an iBWC:

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

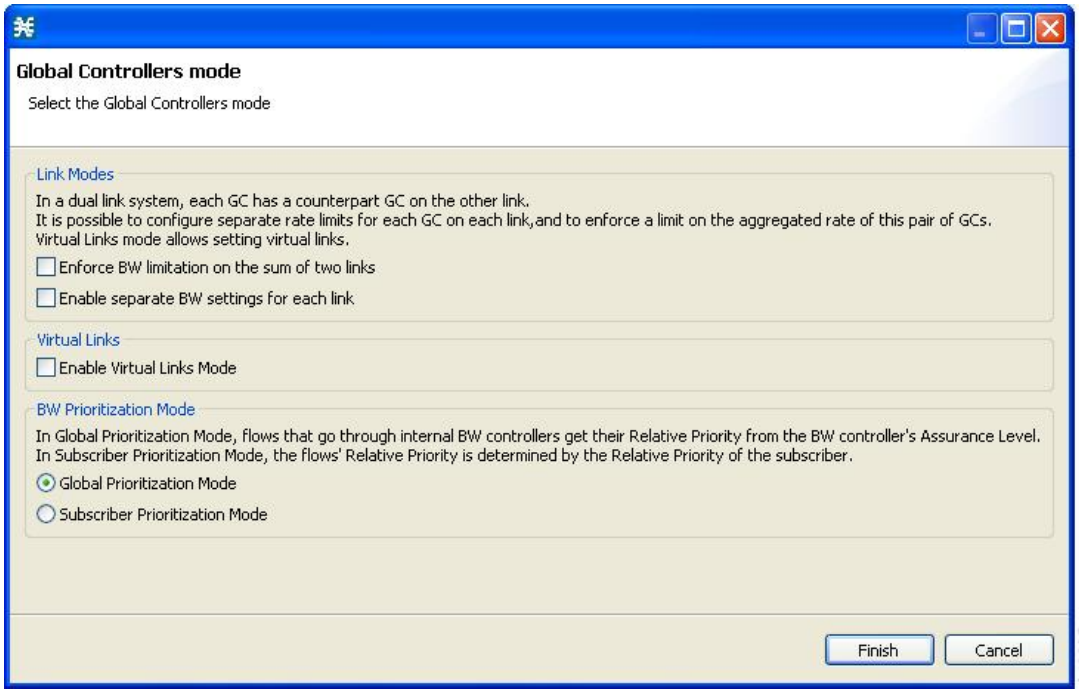
Procedure

Step 1 In the Policies tab, click Global Policy .
The Global Bandwidth Settings are displayed in the right (Rule) pane.

Step 2 Click Edit Preferences .

The Global Controllers mode dialog box appears.

Figure 207: Global Controllers Mode



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

- Global Prioritization Mode
- Subscriber Prioritization Mode

Step 4 Click OK .
The Global Controllers mode dialog box closes.

The selected BW management parameter is saved.

Introduction to Managing Virtual Links

In Virtual Links mode, template bandwidth controllers are defined for packages. Actual bandwidth parameters are assigned when a subscriber enters the system. This bandwidth depends on the package of the subscriber and the physical link assigned to the subscriber. The package of the subscriber defines the template controllers.

For each service configuration that has Virtual Links mode enabled, there is one default upstream virtual link and one default downstream virtual link. The upstream and downstream interfaces are each assigned one default template global controller.

You can add additional template global controllers. You can add, modify, and delete virtual links using a command-line interface (CLI).

The number of directional template global controllers limits the maximum number of virtual links. The number of template global controllers times the number of virtual links cannot exceed 1024 or 4096. Based on the Cisco SCE hardware, the number of global controllers varies. For details, see the Introduction to Managing Bandwidth, on page 269section.

To support the DOCSIS 3.0 Downstream bonding, a two level virtual link hierarchy is created for the wideband channels. The wideband channels are associated with the Aggregate Global Control (AGC) that provides a constant output signal despite variations in input signal strength. Wideband channels are associated with three AGCs in a two level hierarchy. At the lower level of the hierarchy, all the DOCSIS 3.0 modems for wideband are aggregated into one AGC and the other AGC contains both legacy and 3.0 modems. The AGC at the top level of the hierarchy is used to limit the aggregated bandwidth of the wideband channel.

For more information on the support for DOCSIS 3.0 solution, see the Cisco Service Control for Managing Remote Cable MSO Links Solution Guide.

For more information on managing the virtual links global controllers, see the Managing Virtual Links Global Controllers section.

Note If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration. A subscriber BWC that pointed to a user-defined global controller now points to the default global controller. (Other parameters of these subscriber BWCs remain unchanged.)

Note While applying a policy in virtual link mode, if the new template includes a different number of global controllers than the currently applied template, you must choose the Reset all Virtual Links to Template Rate Limits. Otherwise, selecting apply results in en error message, similar to the following: “Template Upstream Virtual Link differ from the one in the SCE - cannot apply without the force template virtual link option.”

Collection Manager Virtual Links Names Utility

The Cisco Service Control Collection Manager includes a command-line utility for managing the names of virtual links.

For more information about the Cisco Service Control Collection Manager Virtual Links Names Utility, see the “Managing Virtual Links” section in the “Managing the Collection Manager” chapter of Cisco Service Control Management Suite Collection Manager User Guide .

Enabling Virtual Links Mode

To use virtual links, you must enable Virtual Links mode.

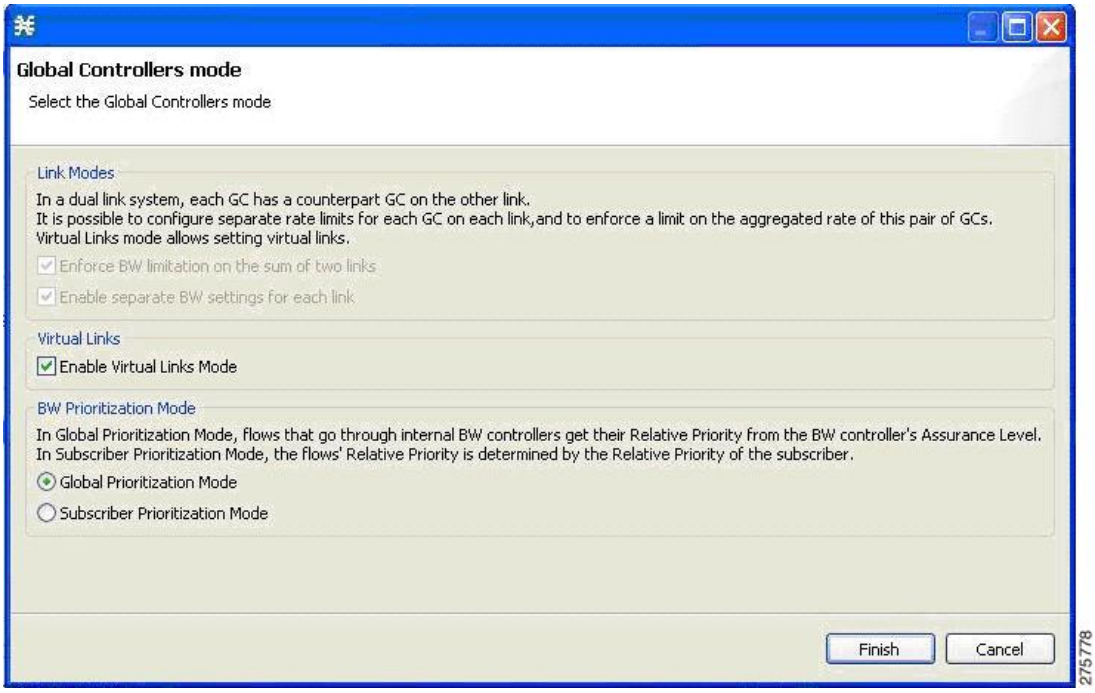
Note If you enable or disable Virtual Links mode, all user-defined global controllers are deleted from the service configuration.

Procedure

Step 1 In the Policies tab, click Global Policy .
The Global Bandwidth Settings are displayed in the right (Rule) pane.

Step 2 Click Edit Preferences .
The Global Controllers mode dialog box appears.

Figure 208: Global Controllers Mode



Step 3 Check the Enable Virtual Links Mode check box.
If you have already added global controllers or if you selected asymmetric routing classification mode, a warning message appears. To continue, click OK .
The Virtual Links Global Controllers tab opens.

Step 4 Click Finish .
The Global Bandwidth Settings dialog box closes.

Viewing Virtual Links Global Controller Settings

Note Global controller bandwidth is based on Layer 1 volume. (Accounting, reporting, and subscriber bandwidth control in Cisco SCA BB is based on Layer 3 volume.)

Procedure

Step 1 In the **Policies** tab, click **Global Policy** .
The Global Bandwidth Settings are displayed in the right (Rule) pane.

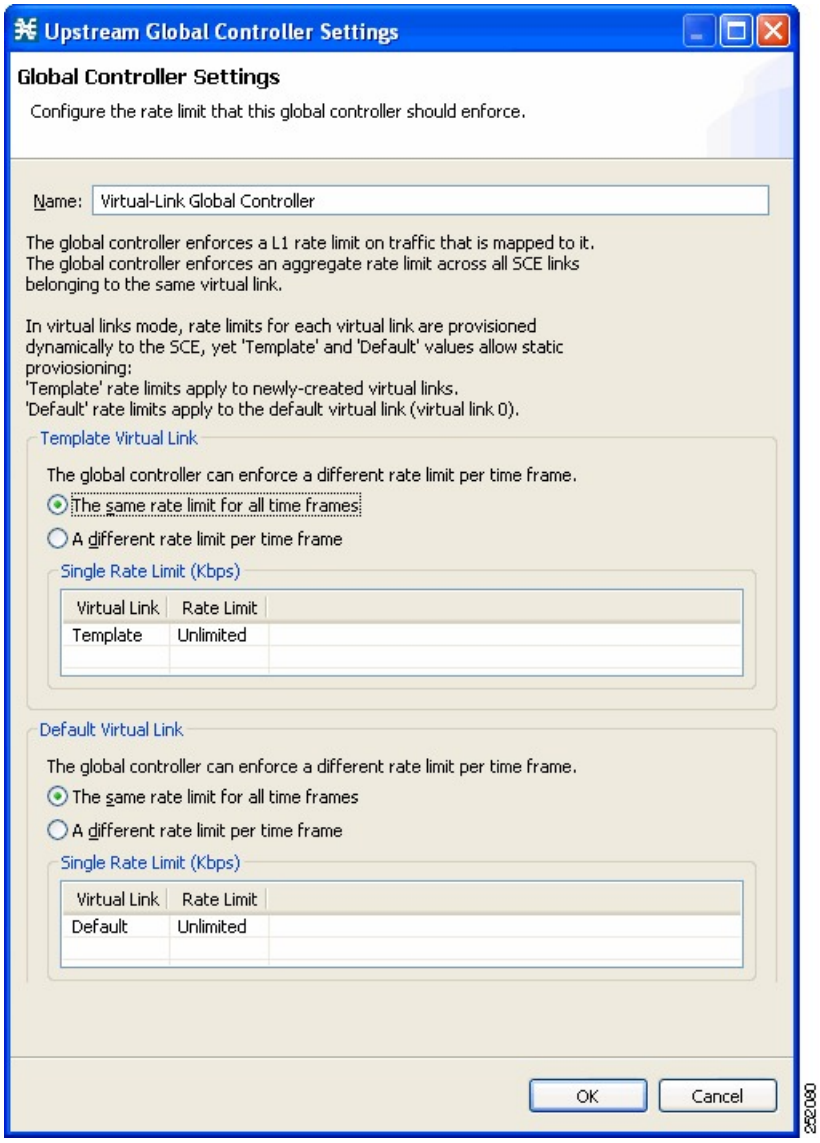
The maximum amount of bandwidth that can be used by any global controller is displayed at the top of the Global Bandwidth Settings:

- Total Link Upstream Bandwidth Limit: Link 1
- Total Link Downstream Bandwidth Limit: Link 1

Step 2 Select a global controller, and click the Edit () icon.

The Global Controller Settings dialog box appears.

Figure 209: Upstream Global Controller Settings



The values of the global controllers defined in the dialog box depends on the values displayed in the Global Bandwidth Settings. So, for example, if the Total Link Upstream Bandwidth Limit: Link 1 has a value of 10 Mbps then the upstream default global controller value cannot exceed 10 Mbps.

The Name field contains a unique name assigned to the global controller. The system automatically assigns the names Controller 1, Controller 2, and so on.

The dialog box contains the following two tabs:

- Template Virtual Link —The default maximum value of the total link limit permitted to global controllers of any created virtual links, either for all time frames or per time frame.

- Default Virtual Link —The maximum value of the total link limit permitted to global controllers of the default virtual link, either for all time frames or per time frame.

Step 3 Click OK.
The Global Bandwidth Settings dialog box closes.

Managing Virtual Links Global Controllers

Virtual link global controllers can be added edited and deleted in the same way as regular global controllers. For more information, see the following sections:

- Adding Global Controllers, on page 310
- Setting the Maximum Bandwidth of Global Controllers, on page 313
- Deleting Global Controllers, on page 314
- Introduction to Defining Global Controllers, on page 274
- Introduction to Managing Subscriber Bandwidth, on page 291

Adding Global Controllers

Based on the Cisco SCE hardware, the number of global controllers you can add to a service configuration varies. For details, see the Introduction to Managing Bandwidth, on page 269 section.

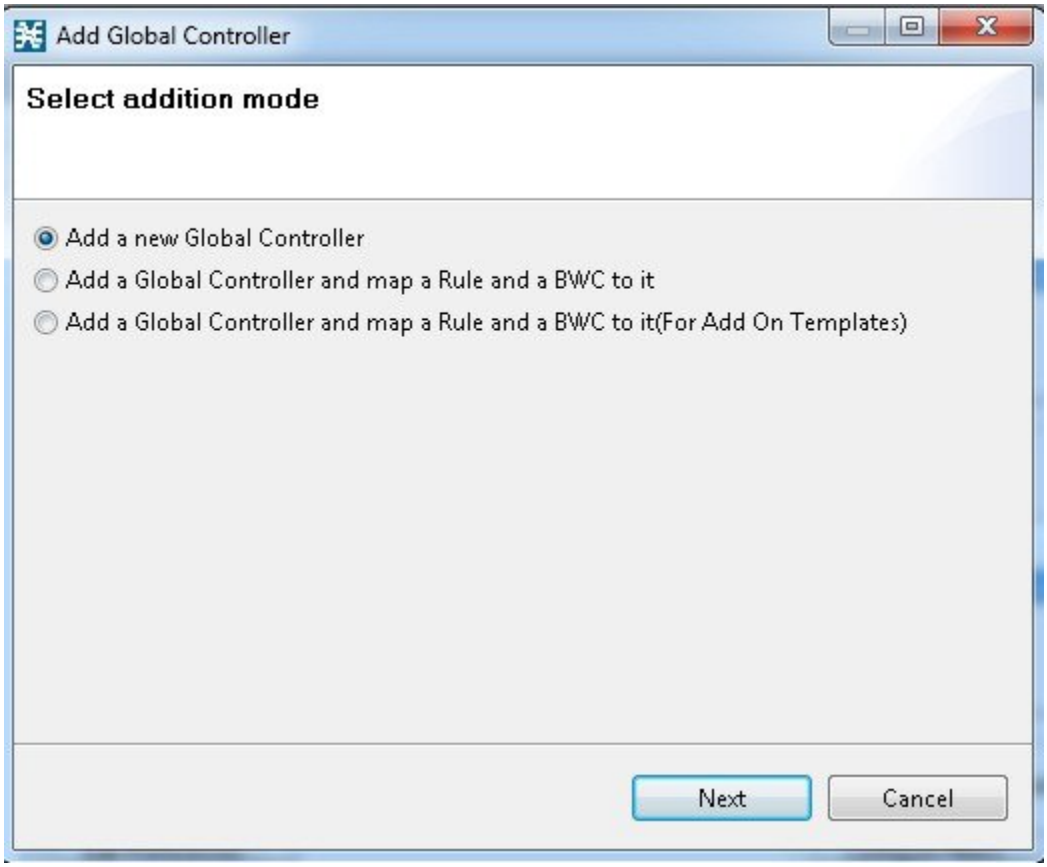
Procedure

Step 1 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

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

The Select Addition mode dialog box appears.

Figure 210: Select Addition Mode

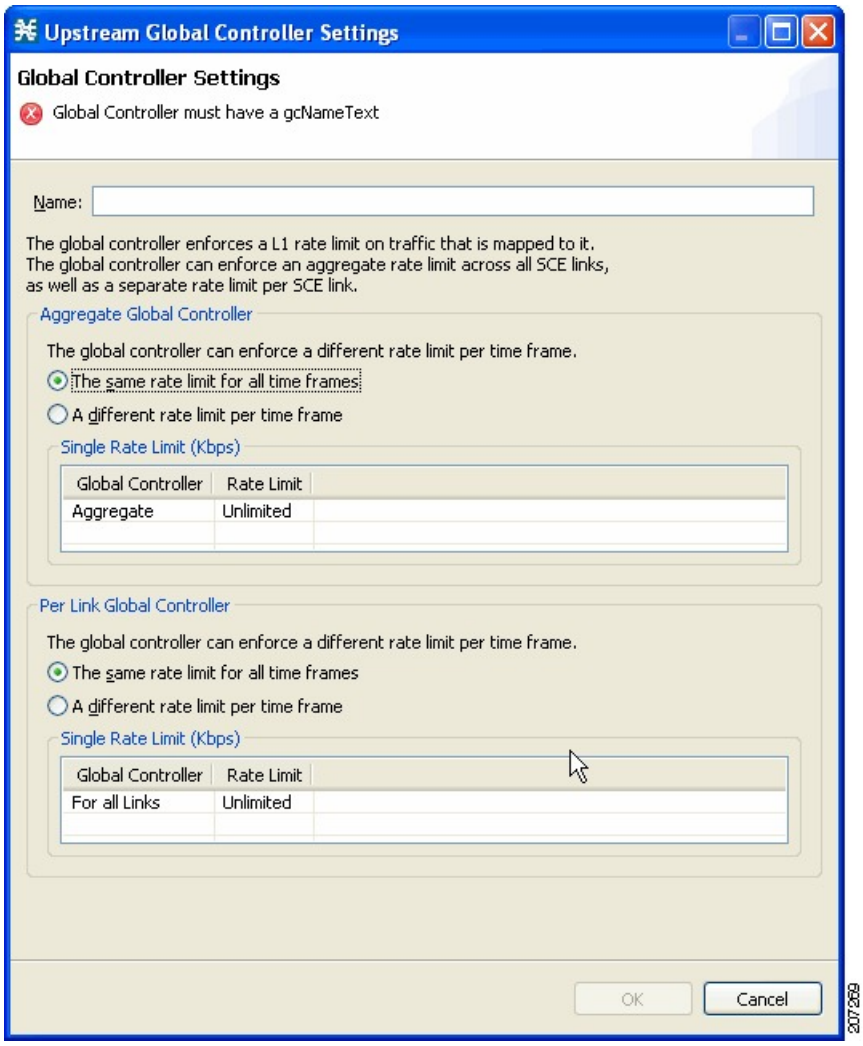


Step 3 Choose the Add a new Global Controller radio button, to add a new global controller.

Step 4 Click Finish.
The Global Controller Settings dialog box appears.

Note The display of Upstream Global Controller Settings depends on the global controller mode setting.

Figure 211: Upstream Global Controller Settings



Step 5 In the Name field enter a meaningful name.

Step 6 To edit the maximum bandwidth of the global controller, continue with the instructions in the section Setting the Maximum Bandwidth of Global Controllers, on page 313.

Step 7 Click OK.
Your changes are saved.

The Global Controller Settings dialog box closes.

Setting the Maximum Bandwidth of Global Controllers

You can edit the maximum bandwidth that a global controller can carry.

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

You can set different values for each link and for the aggregated BW of all links.

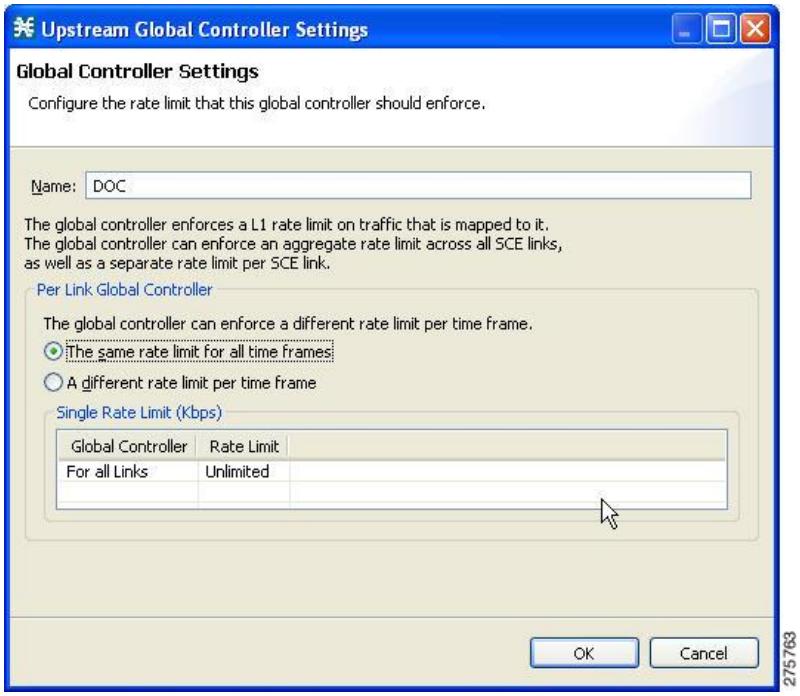
Procedure

Step 1 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 2 Select a global controller.

Step 3 Click the Edit ( ) icon.
The Global Controller Settings dialog box appears.
Note The display depends on the global controller mode setting.

Figure 212: Upstream Global Controller Settings



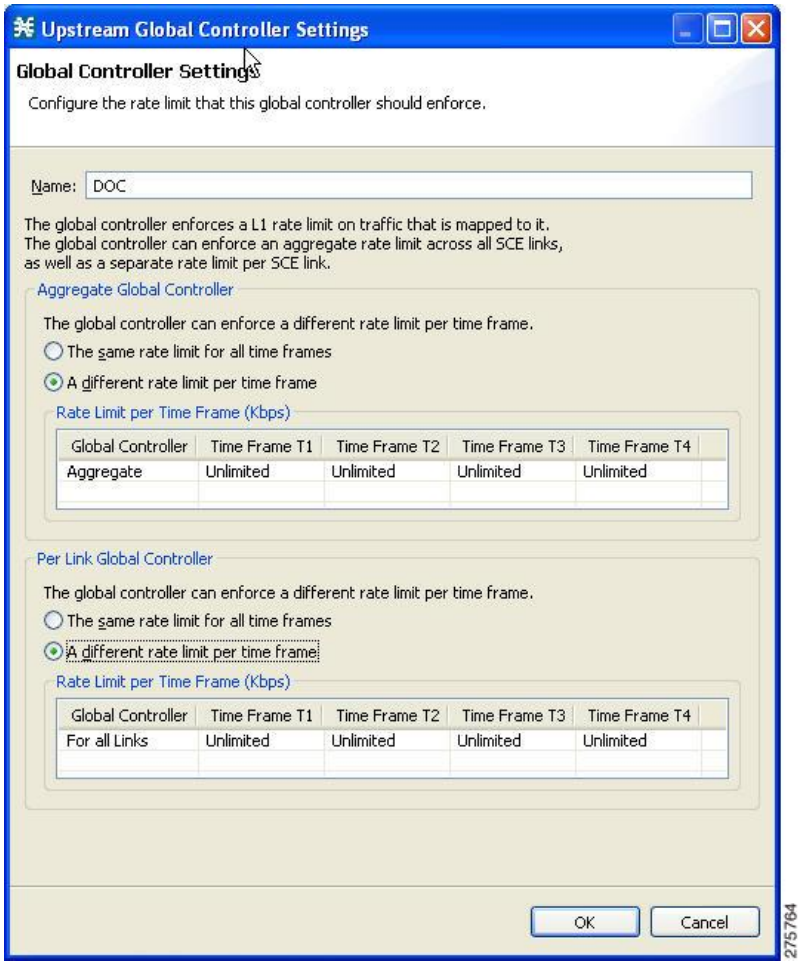
Step 4 Set a single value for the maximum bandwidth limit that this global controller carries.

- Choose the The same rate limit for all time frames radio button, and in the Single Rate Limit (Kbps) field, enter the desired value in Kbps for the maximum bandwidth.

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

Step 6 Choose the A different rate limit per time frame radio button, and enter the desired value for each time frame.
Note The display depends on the global controller mode setting.

Figure 213: Upstream Global Controller Settings



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

Step 7 Click OK .
Your changes are saved.

The value in the Policy Description column changes to reflect the new bandwidth limits.

Step 8 Repeat Step 2 through Step 6 for other global controllers.

Deleting Global Controllers

You can delete unused global controllers at any time. The default global controller and the Total Link Limit cannot be deleted.

Procedure

Step 1 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box appears.

Step 2 Select a global controller.

Step 3 Click the Delete ( ) icon.

Note If a subscriber BWC is using the specified global controller (see Editing Package Subscriber BWCs, on page 292 section), a global controller cannot be removed message is displayed. The global controller cannot be deleted until you unassign it from all subscriber BWCs.

The global controller is deleted.

Step 4 Click OK.
Your changes are saved.

The Global Bandwidth Settings dialog box closes.

Configuring a Service Configuation in Virtual Links Mode

The following steps outline configuring a service configuration in Virtual Links mode. The procedure is similar to that for configuring any service configuration, but virtual links must be added using the CLI.

Procedure

Step 1 Create a new service configuration.

Step 2 Open the **Global Bandwidth Settings** dialog box and check the **Enable Virtual Links Mode** check box.

Step 3 Create template global controllers.

Step 4 Create packages.

Step 5 Add subscriber BW controllers to the packages and associate them with appropriate global controllers.

Step 6 Apply the service configuration.

Step 7 The bandwidth values of the default global controllers are set; the values of all other global controllers are not set – these global controllers are templates.

Step 8 Add virtual links using the CLI.

Each virtual link gets a set of global controllers with the PIR values of the template global controller configuration.

If necessary, you can use the CLI to change the PIR values of the global controller.

1. A subscriber is introduced to the Cisco SCE platform. Upstream and downstream virtual links are associated with the subscriber as well as a package.
2. Rule resolution for each flow of the subscriber is according to the package of the subscriber and the global controller configuration of the virtual link.

Editing the Virtual Links Total Link Limits

You can limit the total bandwidth passing through the physical link.

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

In Virtual Links mode, bandwidth limitations are applied to the sum of all links.

Procedure

Step 1 In the Policies tab, click Global Policy.
The Global Bandwidth Settings dialog box is displayed in the right (Rule) pane.

Step 2 In the Upstream or Downstream section, click Edit Rate Limit .
The Total Rate Limit dialog box appears.

Step 3 In the Total Rate Limit for each SCE link (Kbps) field, enter the maximum bandwidth of the Cisco SCE platform capacity that the platform carries, or enter Unlimited.

Step 4 Click OK.
The Total Rate Limit dialog box closes.

The Total Link Bandwidth Limit: Link 1 field is updated.

Managing Virtual Links with CLI Commands

You can configure, enable, and disable virtual links using the Cisco SCE platform Command-Line Interface (CLI). For more information about the Cisco SCE platform CLI, see the.

- Use the following CLI commands in line interface configuration mode to manage virtual links:
  - **virtual-links index** <*index*> **direction** [**upstream** | **downstream**]
  - **virtual-links index** <*VL index*> **direction** [**upstream** | **downstream**] **gc** <*gc index*> **set-PIR value** <*PIR 1*, *PIR2*, *PIR3*, *PIR4*>
  - **virtual-links index** <*VL index*> **direction** [**upstream** | **downstream**] **gc** <*gc index*> **set-PIR value** <*PIR for all timeframes*>
  - **virtual-links index** <*VL index*> **direction** [**upstream** | **downstream**] **gc** <*gc index*> **reset-PIR**
  - **no virtual-links index** <*index*> **direction** [**upstream** | **downstream**]
- Use the following CLI command in line interface configuration mode to set the virtual links index of a subscriber:
  - **subscriber name** <*name*> **property name** [**vlUp** | **vlDown**] **value** <*vl index*>
- Use the following CLI command in EXEC mode to monitor the status of virtual links:
  - **Show interface LineCard 0 virtual-links** [**all** | **changed** | **different-from-template**]

Description of Virtual Links CLI Commands

Table 10: Virtual Links CLI Commands

Command	Description
virtual-links index <index> direction [upstream | downstream]	Add a virtual link
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR value <PIR 1, PIR2, PIR3, PIR4>	Update the global controller PIR values of a virtual link - separate values for each time frame
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR value <PIR for all timeframes>	Update the global controller PIR values of a virtual link - one value for all time frames
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> reset-PIR	Update the global controller PIR values of a virtual link - take the values defined in the template global controller
no virtual-links index <index> direction [upstream | downstream]	Delete a virtual link
subscriber name <name> property name [vlUp | vlDown] value <vl index>	Set a virtual links index for the subscriber
show interface LineCard 0 virtual-links all	Show information about all virtual links
Show interface LineCard 0 virtual-links [all | changed | different-from-template]	Show information about virtual links whose PIR is changed or differs from the value defined in the template global controller

Entering Line Interface Configuration Mode

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

Procedure

Step 1 At the Cisco SCE platform CLI prompt (SCE#), type configure .

Step 2 Press Enter.
The SCE(config)# prompt appears.

Step 3 Type **interface LineCard 0**.

Step 4 Press Enter.

The SCE(config if)# prompt appears.

Introduction to Managing Packages

A package is a description of subscriber policy. It is a collection of rules that defines the reaction of the system when it encounters flows that are mapped to the service to which the rule is related. It is recommended that you first define services (see Introduction to Managing Services , on page 158 section) and only then add and define packages.

Every Cisco SCA BB service configuration contains a package, the default package, which is the root package and cannot be deleted.

A subscriber is mapped to the default package in one of the following conditions:

- No other package is specifically assigned to the subscriber
- A nonexistent package is assigned to the subscriber.

A service configuration can contain up to 10000 packages.

Note For SCE 8000, it will be 5000 packages.

Package Parameters

The following parameters define a package:

- General parameters:
  - Package Name—A unique name for the package
  - Description—(Optional) A description of the package
- Quota Management parameters:
  - Quota Management Mode—Specifies how the subscriber quotas are managed—by external quota manager or replenished periodically by Cisco SCA BB.
  - Aggregation Period Type—The quota aggregation period used when quotas are replenished periodically.
  - Quota Buckets—16 resource buckets used for quota management.
- Subscriber BW Controllers parameters:
  - Subscriber relative priority—The relative priority given to subscribers of the package at times of Network congestion.
    Separate priorities are defined for upstream and downstream flows.

- Subscriber Bandwidth Controllers—A list of BW controllers (BWCs) that are available to services that are part of the package. Various parameters are defined for each BWC, including a mapping to a global controller.
  Separate BWCs are defined for upstream and downstream flows.

- Advanced parameters:
  - Package Index—The unique number by which the system recognizes a package. Changing the package name does not affect Cisco SCE platform activity. The system provides a default value of the package index. Do not modify this value.
  - Parent Package—The package one level higher in the package hierarchy. The parent package is important when packages share usage counters. The default package is the base of the package hierarchy, and does not have a parent.
  - Package Usage Counter—Used by the system to generate data about the total use by each package. A package can use either an exclusive package usage counter or the package usage counter of the parent package.
    Each usage counter has:
    - A name assigned by the system (based on the package name).

      Note An asterisk is appended to a package usage counter name whenever the counter applies to more than one package.

    - A unique counter index—The system provides a default value of the counter index. Do not modify this value.
    - Calendar—The calendar used as the basis for the time-based rules of the package.
    - VAS Traffic Forwarding Table—The forwarding table used by the package.

These parameters are defined when you add a new package (see Adding Packages, on page 320 section). You can modify them at any time (see Editing Packages, on page 324 section).

Viewing Packages

You can view a hierarchy tree of all existing packages, and you can see a list of services for which specific rules are defined for any selected package.

Procedure

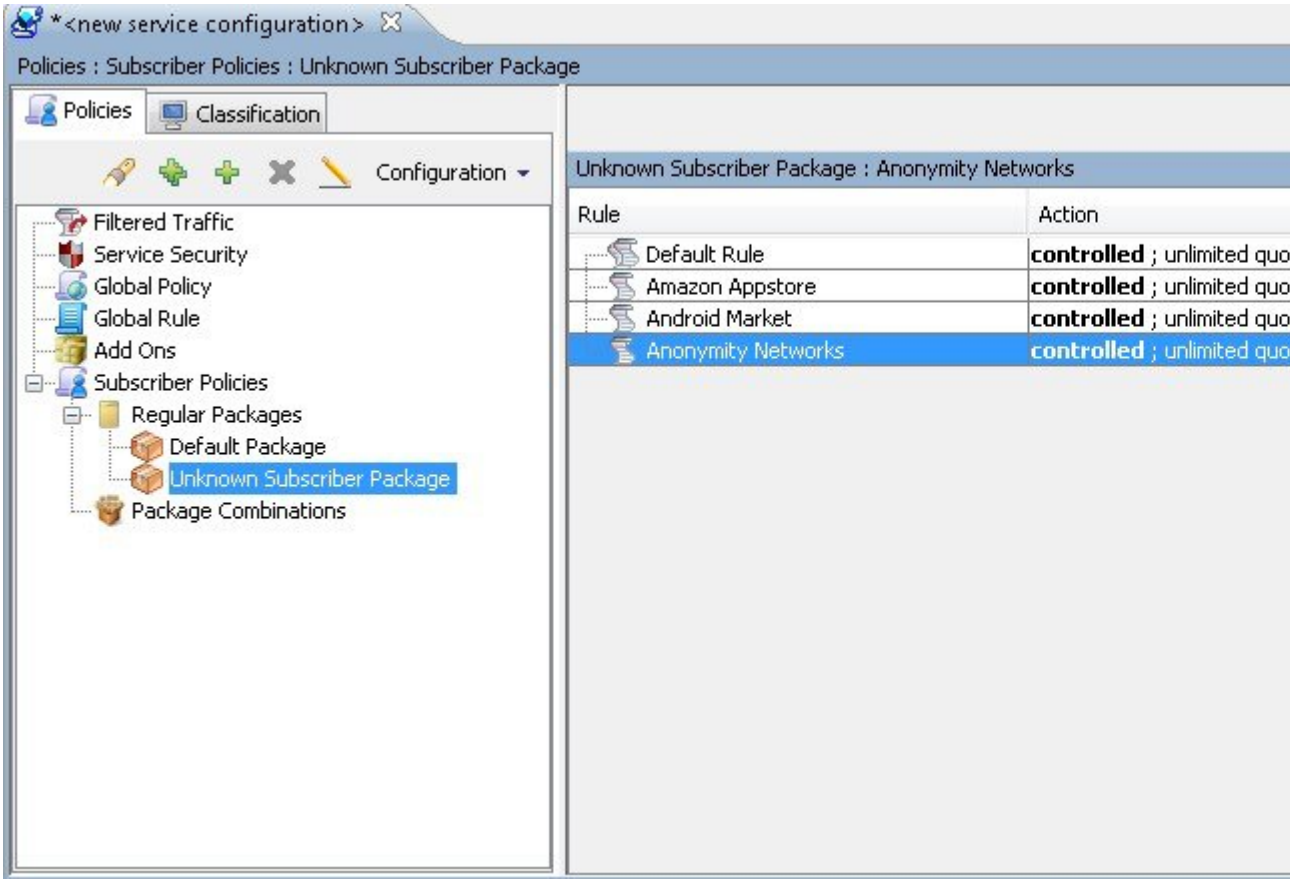
Step 1 In the current service configuration, click the Policies tab.
A list of all packages is displayed in the package tree.

Note To view more information about a package, open the Package Settings dialog box (see Editing Packages, on page 324 section).

Step 2 Click a package in the hierarchy to display the rules of the package.

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

Figure 214: Service Configuration Editor



Adding Packages

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

After you have added a new package, you can define rules for the package (see Adding Rules to a Package , on page 333 section).

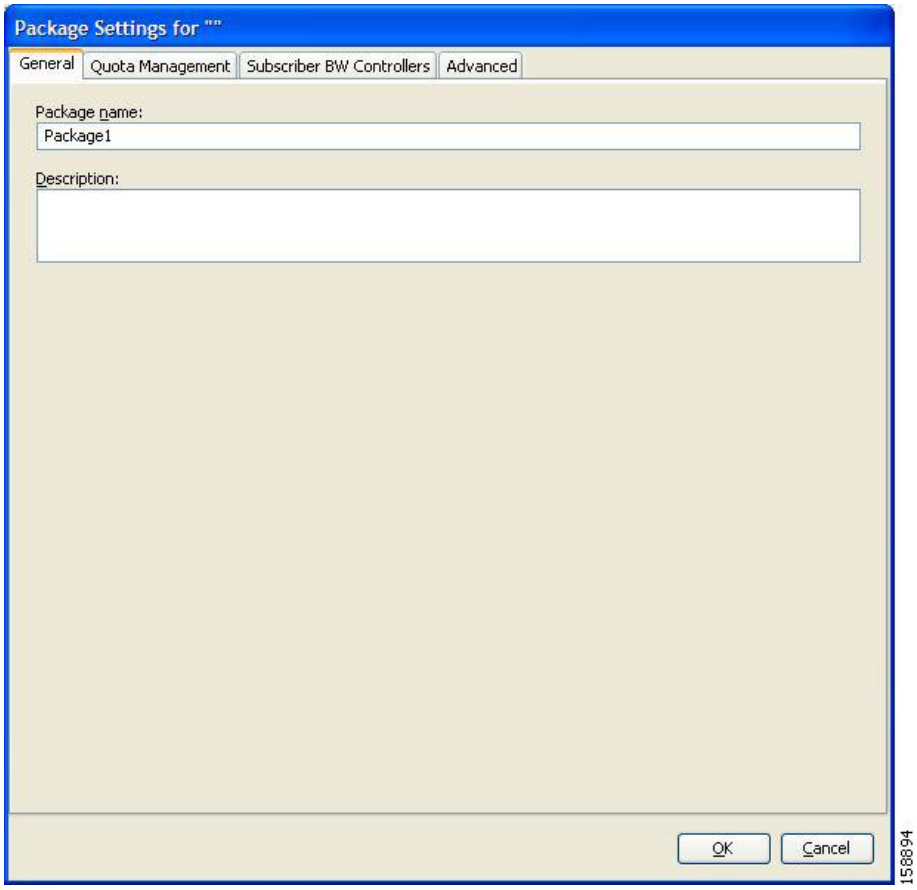
Procedure

Step 1 In the Policies tab, select a package from the package tree. This package is the parent of the package you are adding.

Step 2 In the Policies tab, click the Add Package ( ) icon.

The Package Settings dialog box appears.

Figure 215: Package Settings



Step 3 In the Package name field, enter a unique and relevant name for the package.

Step 4 (Optional) In the Description field, enter a meaningful and useful description of the package.

Step 5 To configure parameters in the Advanced tab, continue with the instructions in the following section.

Step 6 Click OK .
The Package Settings dialog box closes.

The new package is added as a child to the package selected in the package tree and becomes the selected package. The default service rule is displayed in the right (Rule) pane.

What to Do Next

To edit the default service rule, and to add new rules to the package, see Introduction to Managing Rules, on page 331 section.

To configure parameters in the Quota Management tab see Editing Quota Management Settings for Packages , on page 368 section.

To configure parameters in the Subscriber BW Controllers tab, see Editing Package Subscriber BWCs, on page 292 section.

Setting Advanced Package Options

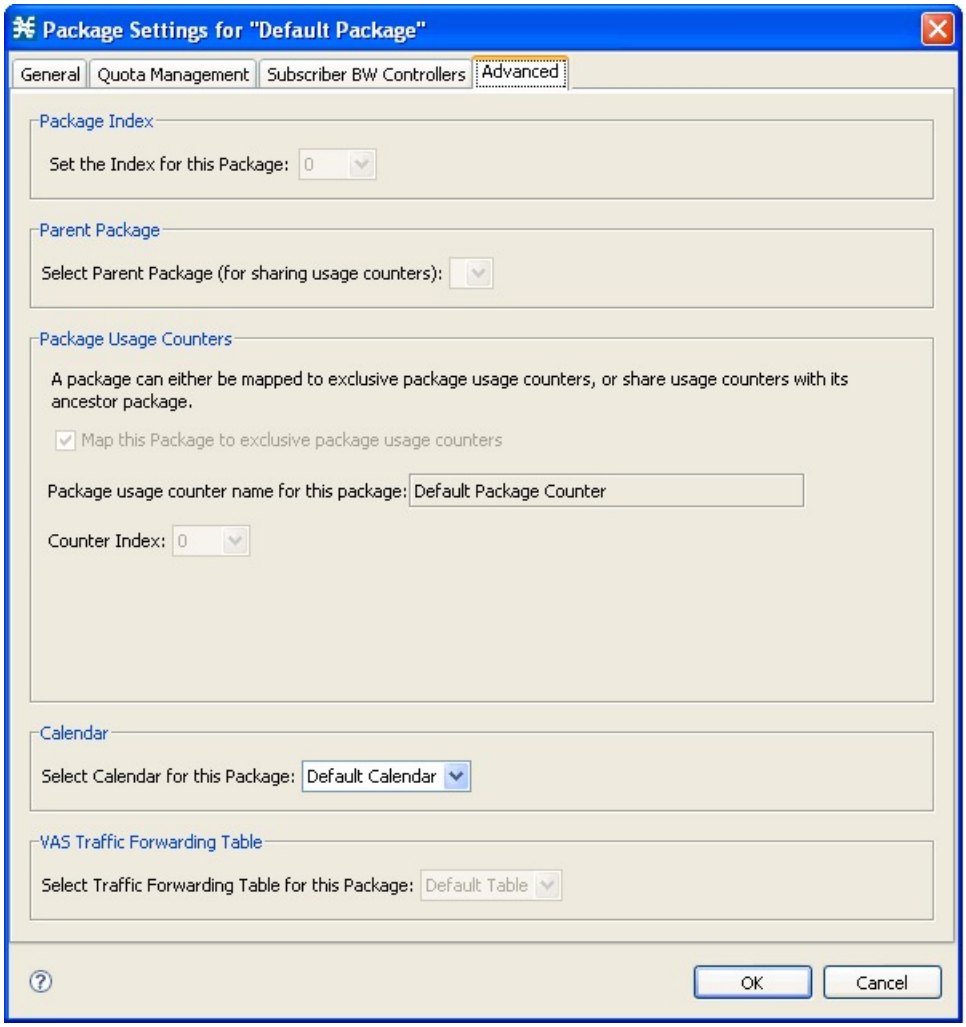
You can change the index for the package, specify an exclusive usage counter, or select a calendar for the package in the Advanced tab.

Procedure

Step 1 In the Package Settings dialog box, click the Advanced tab.

The Advanced tab opens.

Figure 216: Advanced Tab



Step 2 To change the package index for this package, from the Set the Index for this Package drop-down list, select a package index.

Note The system provides a default value of the index. Do not modify this value unless a specific index value must be assigned to the package.

Step 3 To set a different parent package for this package, select the desired parent from the Select Parent Package drop-down list.

Step 4 By default, a new package uses an exclusive usage counter. To share the parent package usage counter, uncheck the **Map this Service to exclusive package usage counters** check box.
The name in the read-only Package usage counter name for this package field changes to reflect your choice.

The Counter Index drop-down list is dimmed.

Step 5 To change the counter index (if you are using an exclusive package usage counter), select a value for the index from the Counter Index drop-down list.

Note The system provides a default value of the index. Do not modify this value.

Step 6 To set a calendar for this package (to use its time frames for time-based rules), select the desired calendar from the Select Calendar for this Package drop-down list.

Step 7 To set a VAS traffic-forwarding table for this package, select the desired traffic-forwarding table from the Select Traffic Forwarding Table for this Package drop-down list.

Note If VAS traffic forwarding is disabled (the default), the drop-down list is dimmed. To enable VAS traffic forwarding, see Enabling VAS Traffic Forwarding, on page 445 section.

Step 8 Click OK.
The Package Settings dialog box closes.

The new package is added as a child to the selected parent package and becomes the selected package. The default service rule is displayed in the right (Rule) pane.

What to Do Next

To edit the default service rule, and to add new rules to the package, see Introduction to Managing Rules, on page 331 section.

Duplicating Packages

Duplicating an existing package is a useful way to create a new package similar to an existing package. It is faster to duplicate a package and then modify it than to define the package from beginning.

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

Procedure

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

Step 2 In the Policies tab, click the Duplicate Package () icon
A duplicate package is created with all the same attributes as the original package. If the package is duplicated several times, the name of the new package is the name of the selected package followed by “(1)”, “(2)”, and so on.

Step 3 Modify the package parameters (see Editing Packages, on page 324 section).

Editing Packages

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

Procedure

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

Step 2 In the Policies tab, click the Edit Package ()icon.
The Package Settings dialog box appears.

Step 3 In the Package name field, enter a new name for the package.

Step 4 In the Description field, enter a new description of the package.

Step 5 (Optional) Change quota management settings, see Editing Package Quota Management Settings (Using the Quota Management Tab (Packages) Editing Quota Management Settings for Packages , on page 368 section.

Step 6 (Optional) (Optional) Change bandwidth control settings, see Editing Package Subscriber BWCs, on page 292 section.

Step 7 To change advanced settings, click the **Advanced** tab.
The Advanced tab opens.

Step 8 To change the package index for this package, from the Set the Index for this Package drop-down list, select a Package Index.

Note The system provides a default value of the counter index. Do not modify this value unless a specific index value must be assigned to the package.

Step 9 To change the parent package of this package, select the desired parent from the Select Parent Package drop-down list.

Step 10 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 11 To use an exclusive package usage counter, check the Map this Service to exclusive package usage counters check box.
The name in the read-only Package usage counter name for this package field changes to reflect your choice.

The Counter Index drop-down list is dimmed.

Step 12 To change the counter index if you are using the exclusive package usage counter, select a value for the index from the Counter Index drop-down list.

Note The system provides a default value of the counter index. Do not modify this value.

Step 13 To change the calendar used by this package, select the desired calendar from the Select Calendar for this Package drop-down list.

Step 14 To change the VAS traffic-forwarding table for this package, select the desired traffic-forwarding table from the Select Traffic Forwarding Table for this Package drop-down list.

Note If VAS traffic forwarding is disabled (the default), the drop-down list is dimmed. To enable VAS traffic forwarding, see Enabling VAS Traffic Forwarding, on page 445 section.

Step 15 Click **OK**.
The Package Settings dialog box closes.

All changes to the package parameters are saved.

Deleting Packages

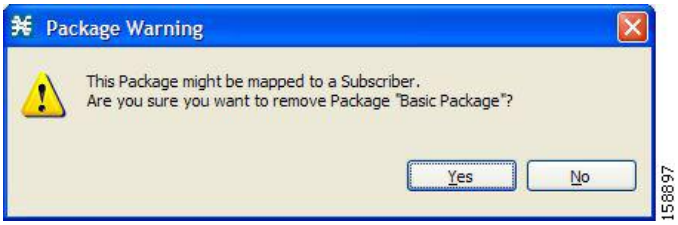
You can delete user-defined packages. The default package cannot be deleted.

Procedure

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

Step 2 In the Policies tab, click the Delete Package ( ) icon.
A Package Warning message appears.

Figure 217: Package Warning



Step 3 Click Yes.
The package is deleted and is no longer displayed in the package tree.

Introduction to Add-on Packages

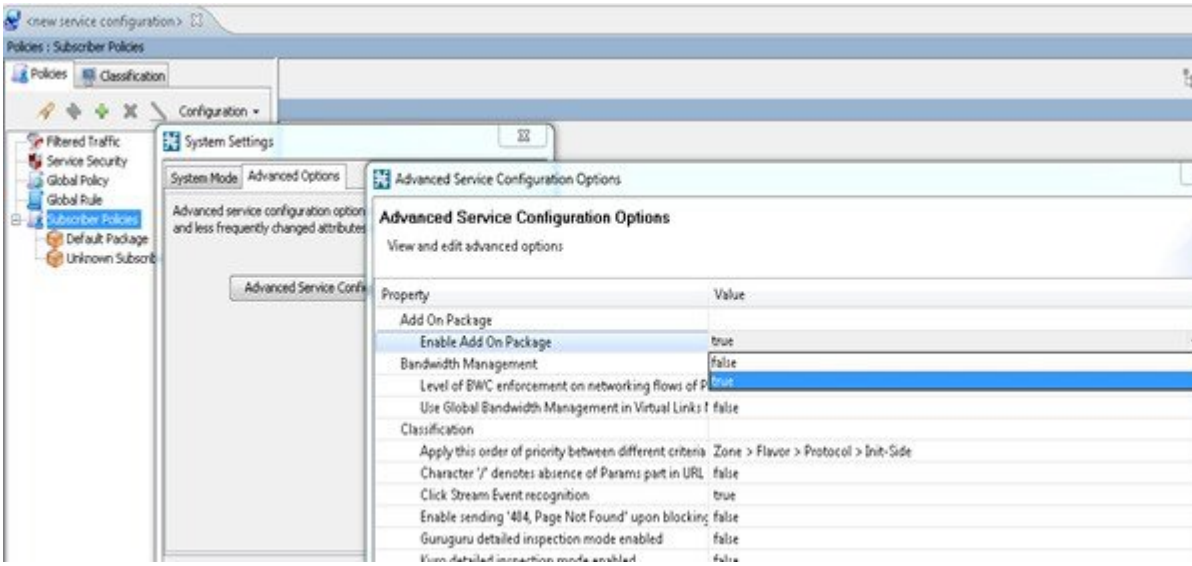
The Add-on Package has been added to Cisco SCABB 5.1 to reduce the complexity of maintaining large number of packages. The package enables you to create up to ten Add-on groups, and add up to 20 Add-on templates under each group.

The three node hierarchies of the Add-on Package are:

- **Add-on Group**, which groups similar templates under one category.
- **Add-on Template**, which is similar to the normal package with the minimal option.

- **Package Combination**, which is a combination of the base package and Add-on Templates that is provisioned to SCE.

Figure 218: Enable Add-on feature



Note Enable Add-on Package under **Configuration > Policies > System Settings > Advanced Options >** Advanced Service Configuration Options before creating Add-on groups.

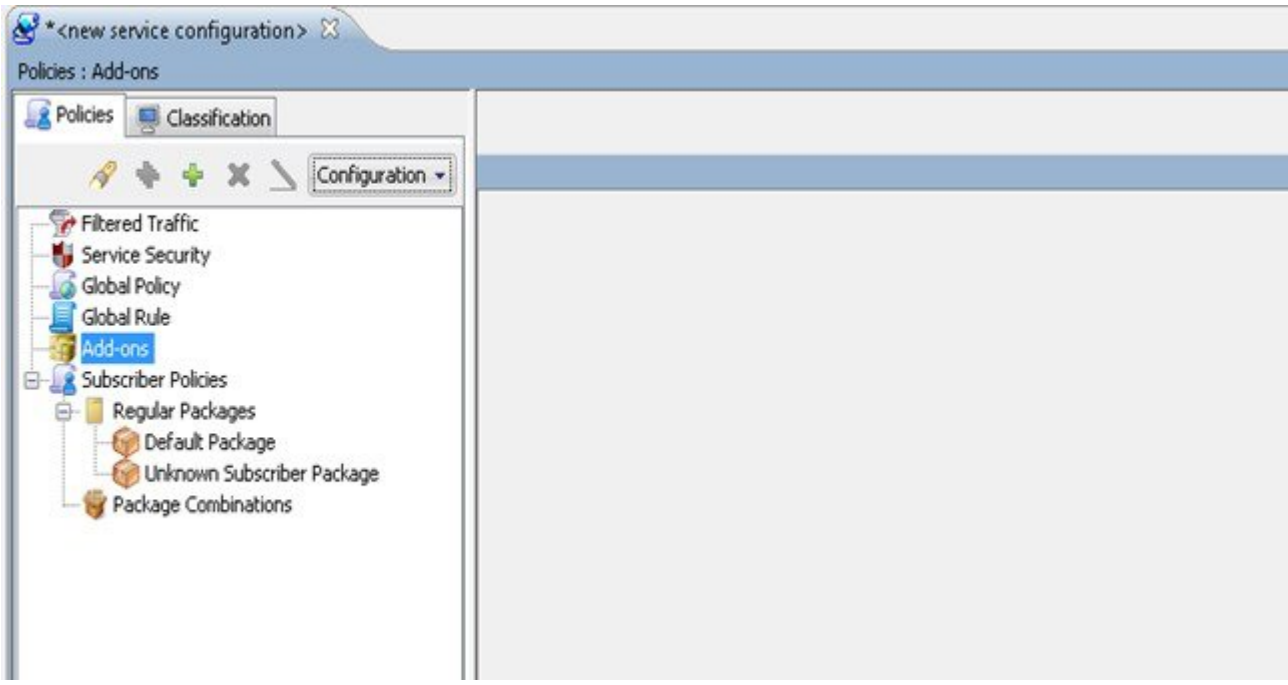
Note Effective with release 5.1.0, SCABB supports Add-on Package solution. This feature is at a nascent stage and will evolve to a complete feature in the future releases of Cisco Service Control Engine. Please contact Cisco Service Control Engine Marketing team for further details and assistance on Add-on package feature.

Adding Add-on Groups

To add the Add-on Groups, follow the below procedure:

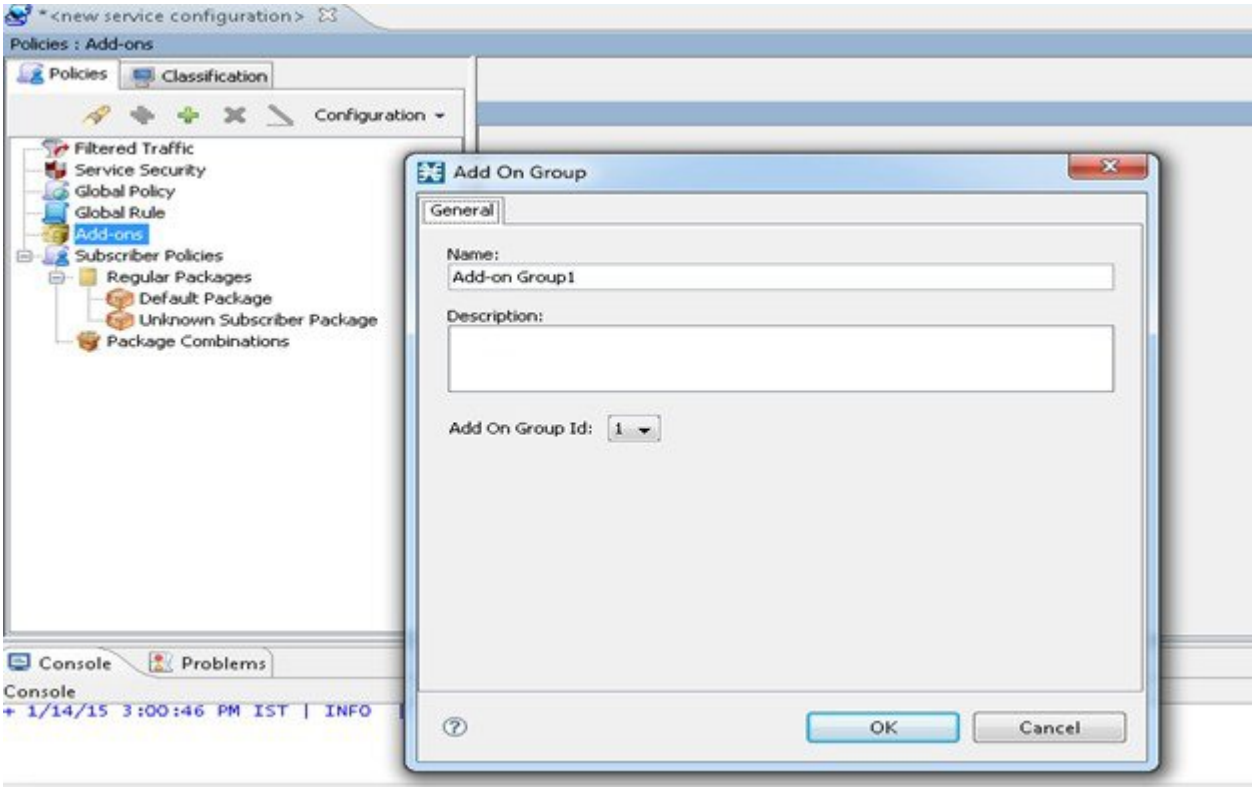
Procedure

Step 1 Navigate to **Service Configuration Editor > Policies > Add-ons**.



Step 2 Select **Add-on > Add-ons Group**.

Figure 219: Creating Add-on Group



Step 3 In the Add-on Group dialog box, enter the name and the description of the group.

Step 4 Select the **Add-on Group Id** from the drop down menu and click **OK** to create the **Add-on Group dialog box.**

Note You can create a maximum of ten Add-on Groups.

Adding Add-on Template

To create an **Add-on Template,** follow the below procedure:

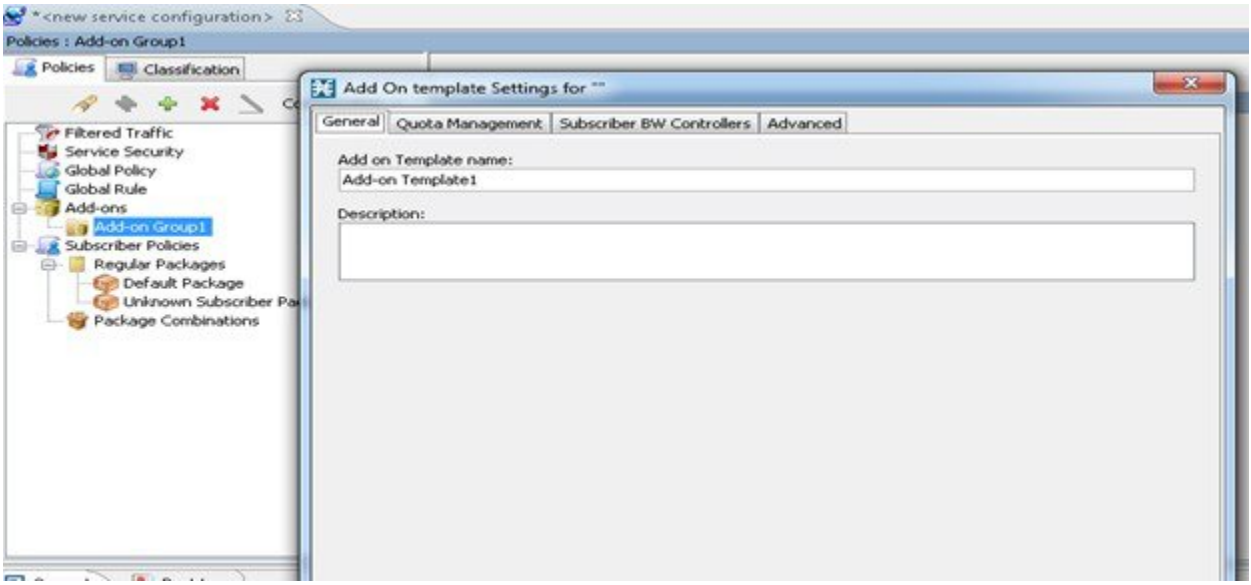
Procedure

Step 1 Navigate to**Service Configuration Editor > Policies >** Add-ons.

Step 2 Navigate to **Add-on Group > Add-ons Group Package**

Step 3 In the Add-on Template dialog box, enter the template name and description.

Figure 220: Creating Add-on template



Step 4 Click the **Quota Management** tab and select the appropriate **Quota Profile** and **Quota Bucket.**

Step 5 Click the **Subscriber BW Controllers** tab and select the Subscriber relative priority for the upstream and downstream BWC.

Note The Subscriber BW Controllers control the bandwidth allotted for transaction groups. They also prioritize the transactions of a single subscriber.

Step 6 Click on the **Advanced** Tab and assign the Index, Calendar and Traffic Forwarding Table for the Add-on Template.

Package Combinations

You can create package combinations using the regular package and Add-on templates under each group. Each package combination must have a base package. Package combinations cannot be repeated. You can filter the Package Combinations based on the Base Package and Add-on Group.

While creating Package Combinations:

- The Package Combination has the Base Package rules. The Add-on Template rules are overwritten in the Package Combination.
- The Package Combination displays the Add-on Template Calendar and VAS settings if the Override option is selected while creating the Add-on template in Advanced tab.
- The Quota Profile of the Add-on Template is overwritten for Package Combination. The Add-on Template quota definition is set to No Override.
- The Bandwidth Controller defined in the Add-on Template is also overridden while creating Package Combinations.
- The Transaction Usage RDR Settings for the Package Combination are based on the TUR option enabled for Add-on template.

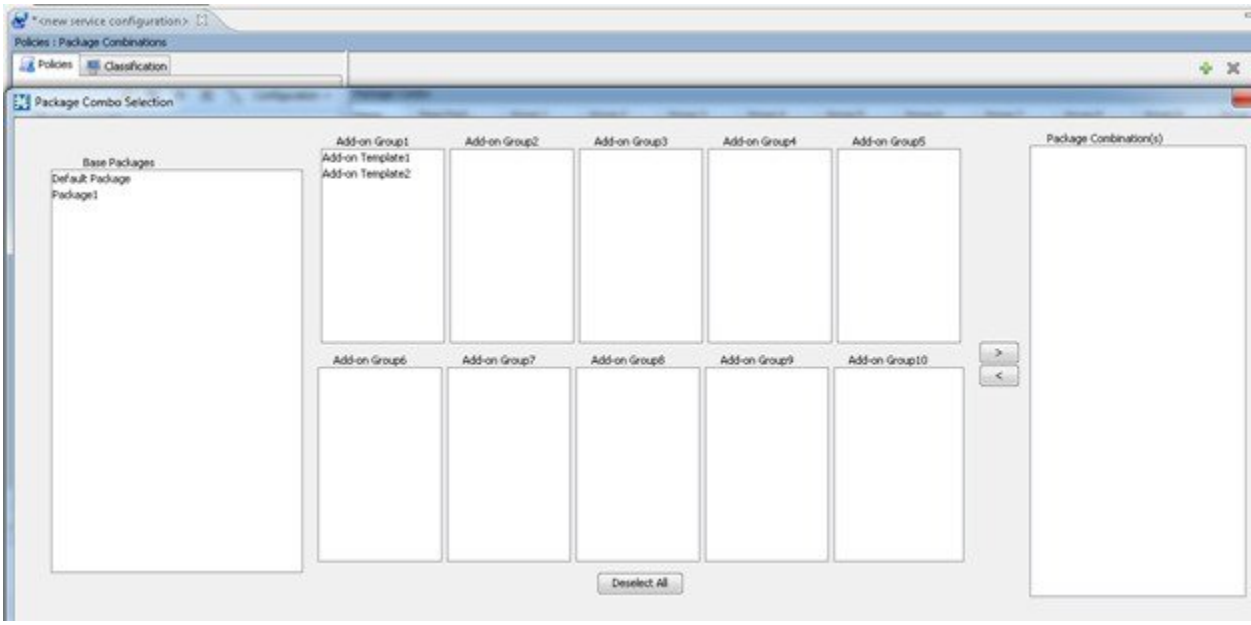
Creating a Package Combination

To create a Package combination, follow the below procedure:

Procedure

Step 1 Navigate to **Service Configuration Editor > Policies > Subscriber Policies > Package Combinations**.

Step 2 Click Add.



Step 3 Select the appropriate package under the base package and the Add-on group.

Note You can create a single package and a template from the respective Base Packages and the Add-on Groups. The Package Combination is validated for conflicting configurations before it is created.

Step 4 Click OK to view the Package Combination displayed under the Package Combo node.

Note You are not allowed to edit the quota management and subscriber BW controllers in the package combinations.

Introduction to Managing Rules

After you have defined services and basic packages, you can define rules for the package.

You can configure rules to do some or all of the following:

- Block the service
- Define maximum bandwidth for the service
- Change the DSCP ToS value of packets in a flow
- Set a quota for the service
- Define behavior when the quota for this service is breached

A rule usually applies at all times. To allow additional flexibility, you can divide the week into four separate time frames. You can define subrules—time-based rules—for each time frame.

Note In Cisco SCA BB, the maximum number of unique rules that can be applied is limited to 5000. If the number of unique rules exceeds the maximum limit, an error occurs. The number of unique rules are identified from the Package ID, Service, and Timeframe fields.

The Default Service Rule

A default service rule is assigned to every package. It cannot be deleted or disabled.

The default values of this rule are:

- Admit (do not block) traffic.
- Map traffic to the default BWCs.
- Do not limit quotas for either upstream or downstream traffic.

Rule Hierarchy

The Cisco SCE platform applies the most specific rule to any flow.

For example, if you define rules for E-Mail and POP3:

- Any flow mapped to the SMTP or IMAP service is handled according to the e-mail rule.
- Any flow mapped to the POP3 service is handled according to the POP3 rule

This means, for example, that POP3 can have its own usage limits, whereas SMTP and IMAP must share usage limits.

Note If you add a rule for a child service, the settings for the parent rule are not copied to the new rule. All new rules start with default values.

 Indicates any rule that also applies to child services.

 Indicates any rule that does not apply to any child services.

Indicates a global rule.

 Time-based rules are shown as children of the relevant rule. The icon for a time-based rule also shows if the rule applies to child services (or).

See also “How to Display the Services Affected by a Rule” section.

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 to which the rule applies, whether the rule is enabled or disabled, and a brief description of the rule.

Procedure

In the Policies tab, select a package from the package tree.
A list of all rules defined for this package is displayed in the right (Rule) pane.

Figure 221: Service Configuration Editor



What to Do Next

To see more information about a rule, open the Edit Rule for Service dialog box (see “How to Edit Rules” section).

To see more information about a time-based rule, open the Edit Time-Based Rule for Service dialog box (see “How to Edit Time-Based Rules” section).

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 How to Add Time-Based Rules to a Rule.

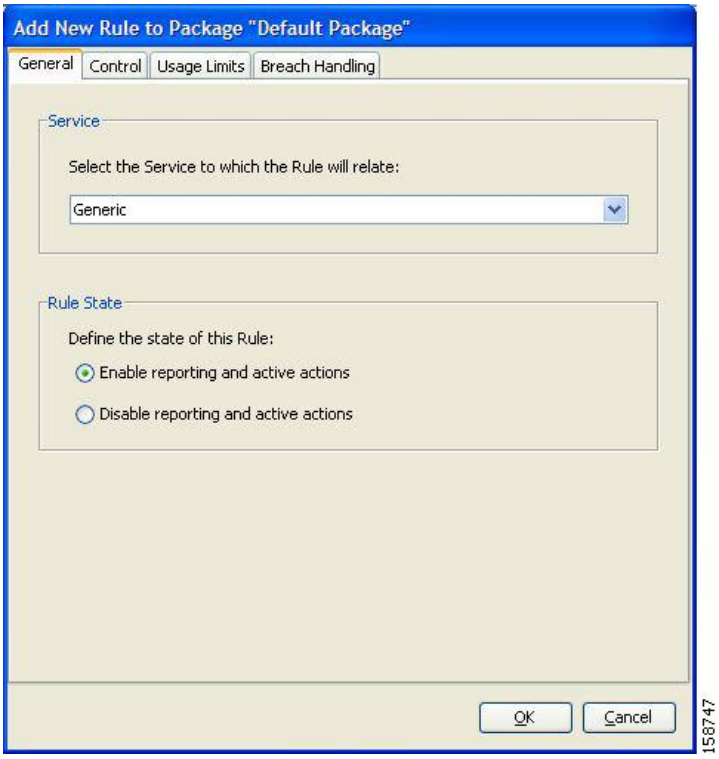
Procedure

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

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

The Add New Rule to Package dialog box appears.

Figure 222: Add New Rule to Package



Step 3 In the Service area of the Add New Rule to Package dialog box, select a service from the Select the Service to Which the Rule Relates drop-down list.

Note Services for which a rule is already defined for this package are dimmed.

Step 4 In the Rule State area, select one of the Define the State of this Rule radio buttons.

- Enable reporting and active actions
- Disable reporting and active actions

Note You can enable or disable a rule at any time (see "How to Edit Rules" section).

Step 5 (Optional) To set behavior per traffic flow for this rule, continue with the instructions in the "How to Define Per-Flow Actions for a Rule" section.

Step 6 Click OK.
The Add New Rule to Package dialog box closes.

The new rule is added to the list of rules displayed in the right (Rule) pane.

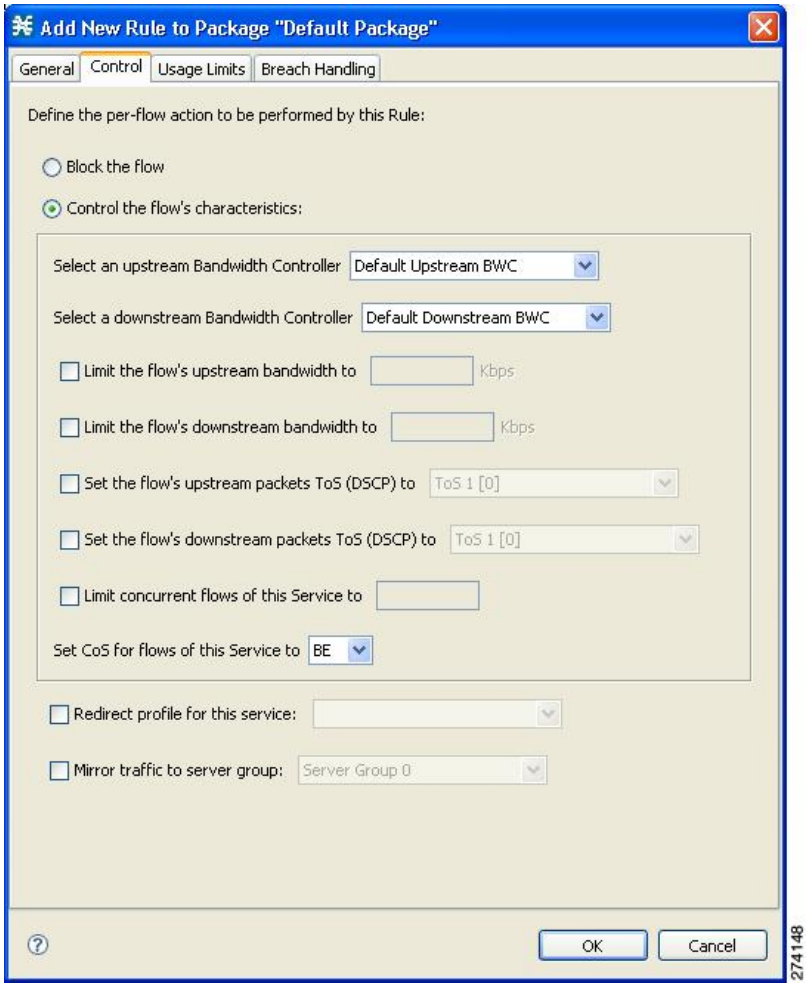
Defining Per-Flow Actions for a Rule

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.

Procedure

Step 1 In the Add New Rule to Package dialog box, click the Control tab.
The Control tab opens.

Figure 223: Control Tab



To control flows that are mapped to the service of this rule, continue at Step 3.

Step 2 To block flows that are mapped to the service of this rule, select the Block the flow radio button and continue at Step 12.

Step 3 Select the Control the flow's characteristics radio button.

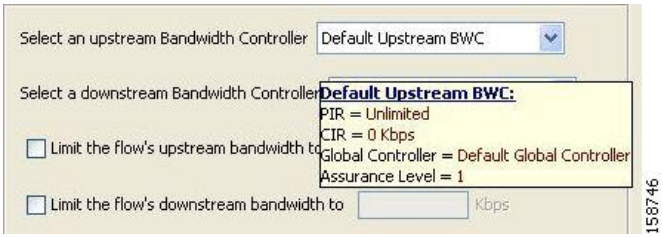
The options in the Flow Characteristic area are enabled.

Step 4 From the upstream Bandwidth Controller drop-down list, select an upstream BWC. This sets up bandwidth metering of all concurrent flows mapped to this rule, based on the characteristics of the selected BWC. The BWCs in this drop-down list are defined when creating or editing the package.

Note For time-based rules: If you need different global controller settings for different time frames, define maximum bandwidths per time frame for one global controller. Do not create a separate global controller for each time frame.

When the mouse is placed over the drop-down list, a tooltip appears (Figure 9-51). The tool tip contains the properties of the selected BWC, such as Peak Information Rate [PIR], Committed Information Rate [CIR], Global Controller, and Assurance Level.

Figure 224: Drop-Down List Tips



Step 5 From the downstream Bandwidth Controller drop-down list, choose a downstream BWC.

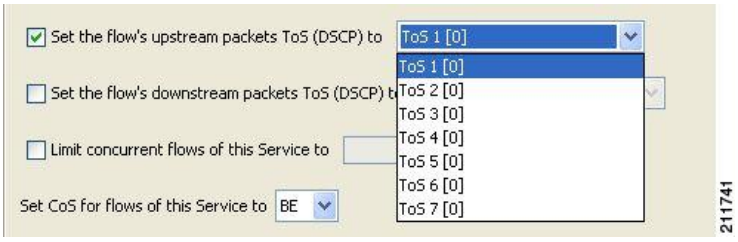
Step 6 (Optional) To set a per-flow upstream bandwidth limit, check the Limit the flow's upstream bandwidth check box and enter a value in the Kbps field.

Note Per-flow bandwidth has a granularity of 1 Kbps up to 57 Mbps.

Step 7 (Optional) To set a per-flow downstream bandwidth limit, check the Limit the flow's downstream bandwidth check box and enter a value in the Kbps field.

Step 8 (Optional) To change the DSCP ToS marker of all packets in upstream flows, check the Set the flow's upstream packets ToS (DSCP) to check box and select a value from the drop-down list.

Figure 225: Drop Down List Values



Step 9 (Optional) To change the DSCP ToS marker of all packets in downstream flows, check the Set the flow's downstream packets ToS (DSCP) to check box and select a value from the drop-down list.

Step 10 (Optional) To set the maximum number of concurrent flows (mapped to this rule) permitted to a subscriber, check the Limit concurrent flows of this Service check box and enter a value in the associated field.

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

Step 12 (Optional) To enable subscriber redirection, check the Redirect profile for this service check box and choose a redirect profile from the drop-down list.

Step 13 (Optional) To enable traffic mirroring, check the Mirror traffic to server group check box and choose a server group from the drop-down list.

Note The Mirror traffic to server group check box is only enabled when Traffic Mirroring is enabled in the VAS Settings dialog box.

Step 14 Click OK.

The Add New Rule to Package dialog box closes.

The new rule is added to the list of rules displayed in the right (Rule) pane.

Editing Rules

You can edit any rule, including the default service rule.



Note You cannot disable the default service rule.



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

Procedure

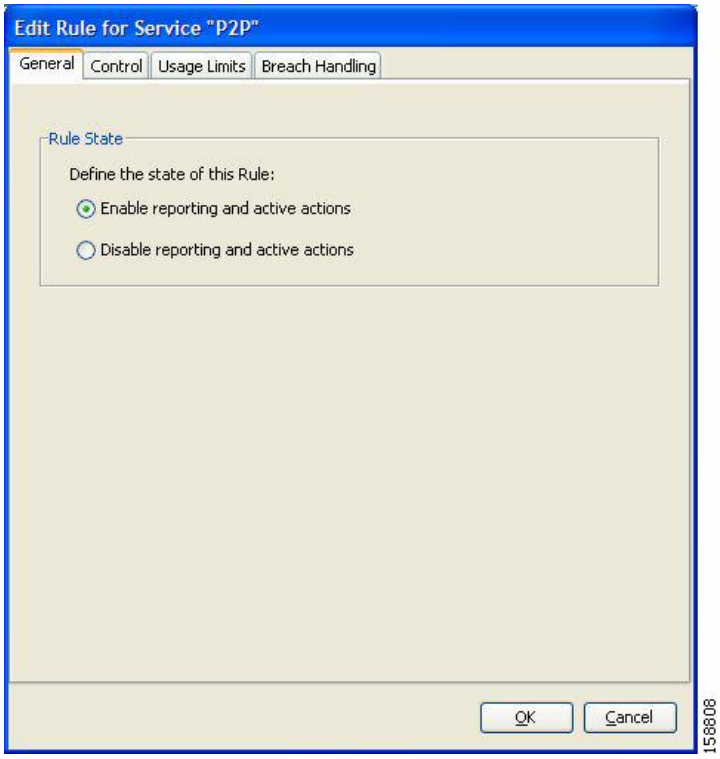
Step 1 In the Policies tab, select a package from the package tree.

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

Step 3 Click Edit Rule.

The Edit Rule for Service dialog box appears.

Figure 226: Edit Rule for Service



Note If you edit a global rule, it becomes a normal rule for that package.

Step 4 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- Enable reporting and active actions
- Disable reporting and active actions

Step 5 Change behavior per traffic flow.

Step 6 Click the **Control** tab.
The Control tab opens.

Step 7 Follow the instructions in Defining Per-Flow Actions for a Rule section.

Step 8 Change usage limits.

Step 9 Click the **Usage Limits** tab.
The Usage Limits tab opens.

Step 10 Follow the instructions in Selecting Quota Buckets for Rules section.

Step 11 Define behavior when a quota is breached.

Step 12 Click the **Breach Handling** tab.
The Breach Handling tab opens.

Step 13 Follow the instructions in Editing Breach-Handling Parameters for a Rule section.

Step 14 Click **OK**.
The Edit Rule for Service dialog box closes.

All changes to the rule are saved.

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. For details, see Step 4 of "How to Edit Rules" section. This feature allows you to enable the rule again later, without having to reset all its parameters. You cannot disable the default service rule.

Procedure

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

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

Step 3 In the Rule pane, click the Delete Rule icon.
A Rule Warning message appears.

Step 4 Click Yes.
The selected rule is deleted.

Displaying the Services Affected by a Rule

You can define a service as the child of another service (the parent service is a service group).

Until you define a separate rule for a child service, the rule of the parent service applies to the child service. A rule that affects any of child services of a service is indicated in the rules list by a different icon, as illustrated for the P2P rule and the FTP rule in.

Figure 227: Rules



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

Note The default service rule applies to all services for which a specific rule is not defined.

Procedure

Step 1 In the right (Rule) pane of the Policies tab, select a rule and click the Show All Services Affected By This Rule.
The Services Affected dialog box appears.

Step 2 Click OK.
The Services Affected dialog box closes.

Global Rules

Effective with Cisco SCE Release 4.1.0, you can define global rules. Using global rules, you can create a rule and apply it to multiple packages. If you modify a global rule, the changes you make affects all its associated packages. You can create upto 10 rules definitions per service.

Adding Global Rules

To create a single service rule definition under a global rule, perform these steps:

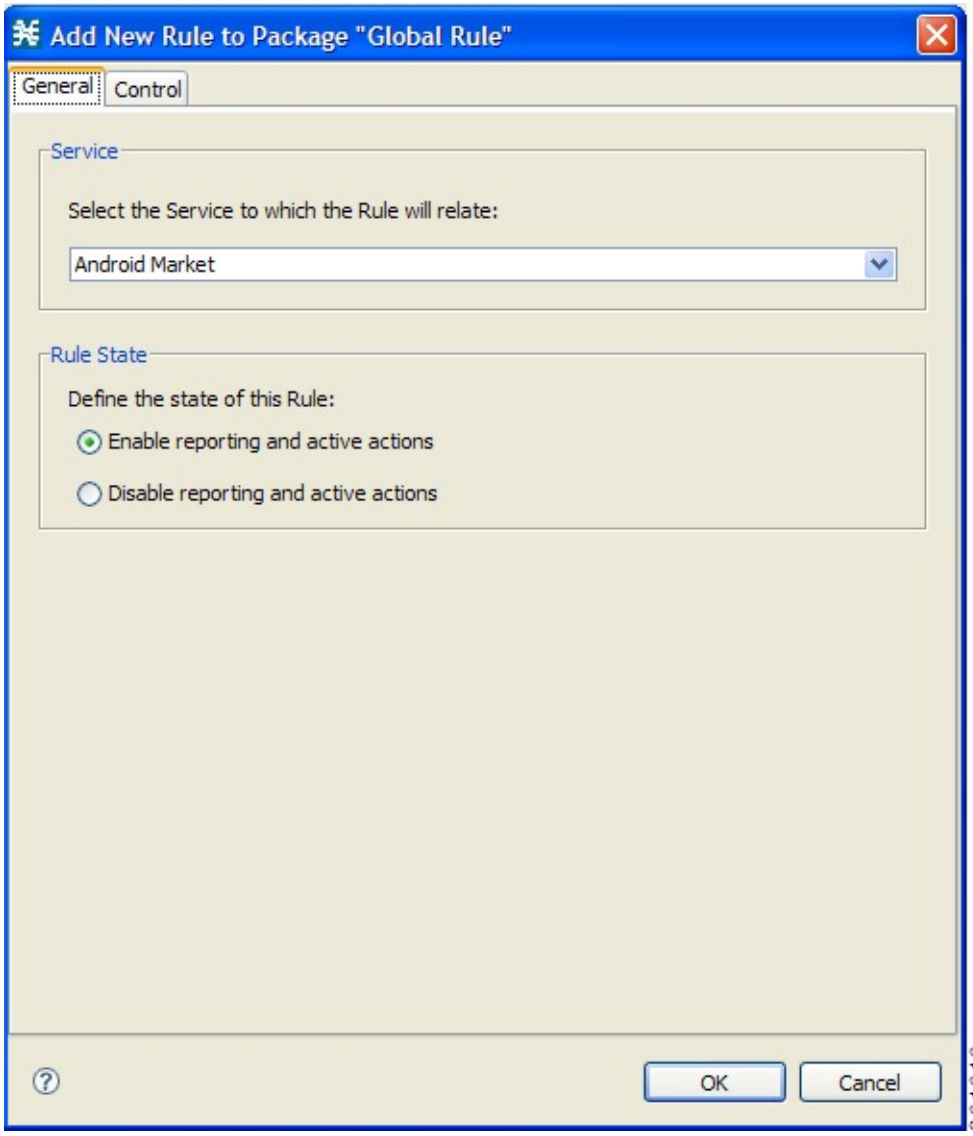
Procedure

Step 1 Under the Policies tab, click **Global Rule**.

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

The Add New Rule to Package Global Rule dialog box appears.

Figure 228: Add New Rule to Package "Global Rule"



Step 3 In the Service area of the Add New Rule to Package Global Rule dialog box, select a service from the Select the Service to Which the Rule Relates drop-down list.

Note Services for which a rule is already defined are dimmed.

Step 4 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- **Enable reporting and active actions**
- **Disable reporting and active actions**

Step 5 (Optional) To set behavior per traffic flow for this rule, continue with the instructions in the Defining Per-Flow Actions for a Rule section.

Step 6 Click **OK**.
The Add New Rule to Package Global Rule dialog box closes.

The new rule is added to the list of rules displayed in the right (Rule) pane.

Editing a Global Rule

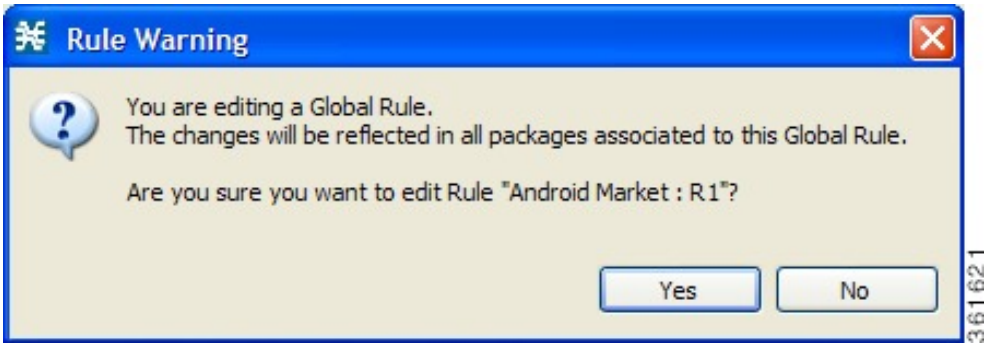
If you edit a global rule, the changes are reflected in all the associated packages.

Procedure

Step 1 Under the Policies tab, click **Global Rule**.

Step 2 Double-click the service rule that you want to edit or click the rule and click the **Edit Rule** button.
A Rule Warning message appears.

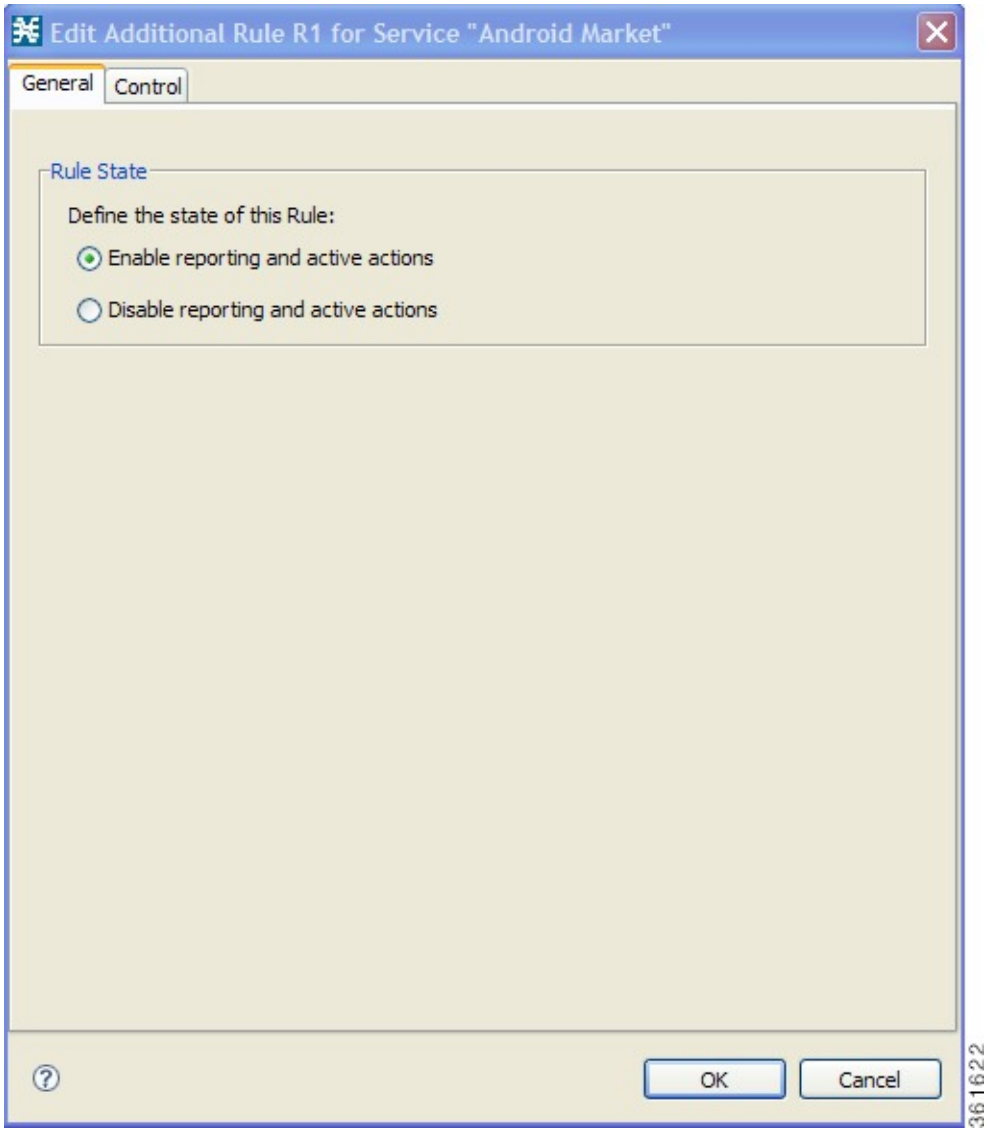
Figure 229: Edit a Global Rule Warning



Step 3 Click **Yes**.

The Edit Additional Rule dialog box appears.

Figure 230: Edit Additional Rule



Step 4 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- **Enable reporting and active actions**
- **Disable reporting and active actions**

Step 5 Change behavior per traffic flow.

Step 6 Click the **Control** tab.
The Control tab opens.

Step 7 Follow the instructions in How to Define Per-Flow Actions for a Rule.

Step 8 Click **OK**.
The Edit Rule for Service dialog box closes.

All changes to the rule are saved.

Adding Additional Global Rules for a Service

After creating a service rule definition under a global rule, you can optionally create more rule definitions for a service. To create more rule definitions for a service, perform these steps:

Procedure

Step 1 Under the Policies tab, click **Global Rule**.

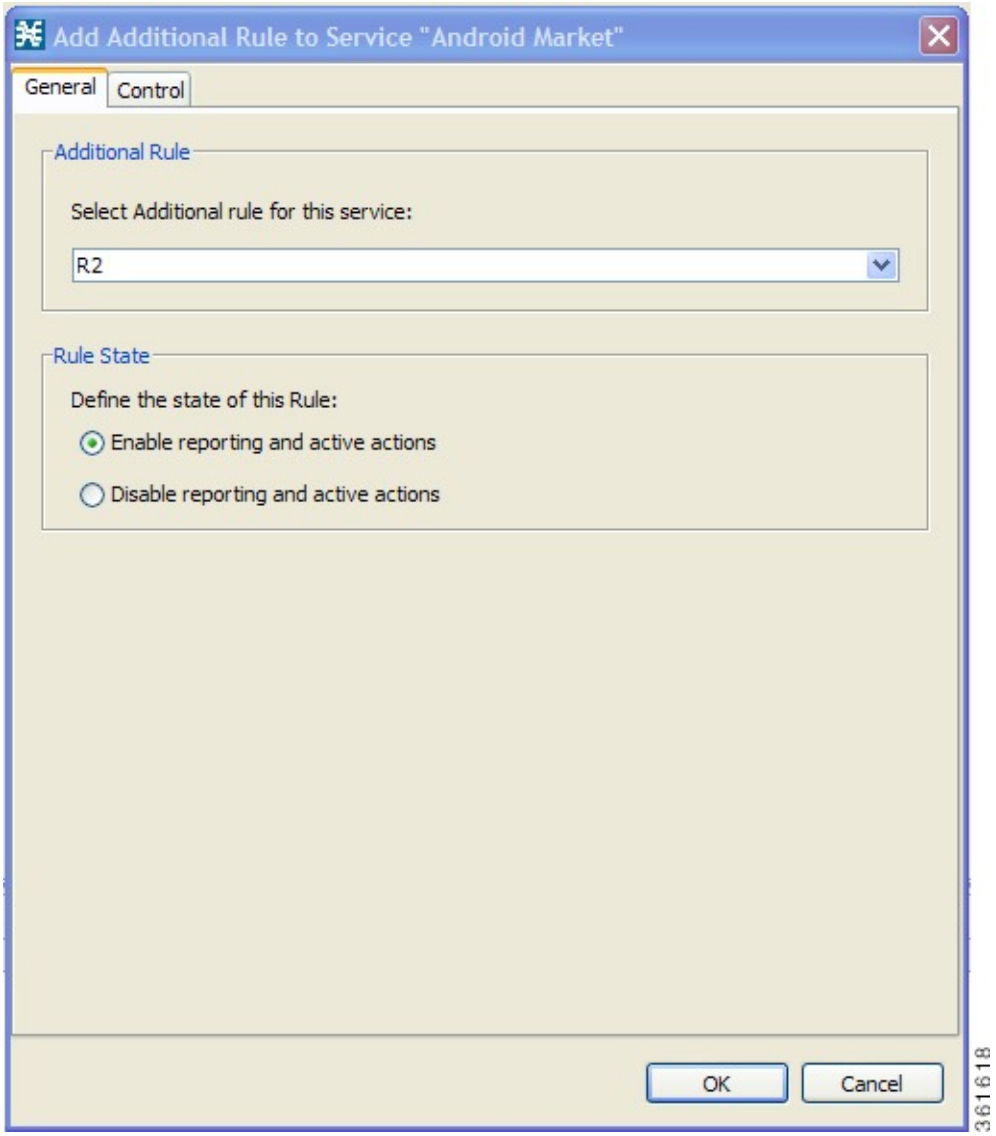
Step 2 Click the service rule to which you want to add additional rules.

Step 3 Click the **Add Additional Rule**  button.

The Add Additional Rule to Package “Global Rule” dialog box appears.

Step 4 In the Additional Rule area, select an additional rule from the Select Additional rule for this service drop-down list.

Figure 231: Add Additional Rule to Service



Note Rules that are already defined are dimmed. You can create upto 10 additional rules.

Step 5 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- **Enable reporting and active actions**
- **Disable reporting and active actions**

Step 6 (Optional) To set behavior per traffic flow for this rule, continue with the instructions in the Defining Per-Flow Actions for a Rule section.

Step 7 Click **OK**.
The Add Additional Rule to Package "Global Rule" dialog box closes.

The new additional rule is added to the list of rules displayed in the right (Rule) pane.

Deleting a Global Rule from a Service

Procedure

Step 1 In the Policies tab, click **Global Rule**.

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

Step 3 In the Rule pane, click the **Delete Rule** icon.
A Rule Warning message appears.

Figure 232:



Step 4 Click **Yes**.
The selected rule is deleted.

Deleting All Additional Rules from a Service

Procedure

Step 1 In the Policies tab, click **Global Rule**.

Step 2 In the right (Rule) pane, select a service to delete.

Step 3 In the Rule pane, click the **Delete Rule** icon.

A Rule Warning message appears.

Figure 233: Delete Global Rule From a Service Warning 1



Step 4 Click **Yes**.
A Rule Warning message appears again.

Figure 234: Delete Global Rule From a Service Warning 2



Step 5 Click **Yes**.
All the global rules associated with the service are deleted.

Adding a Global Rule to a Package

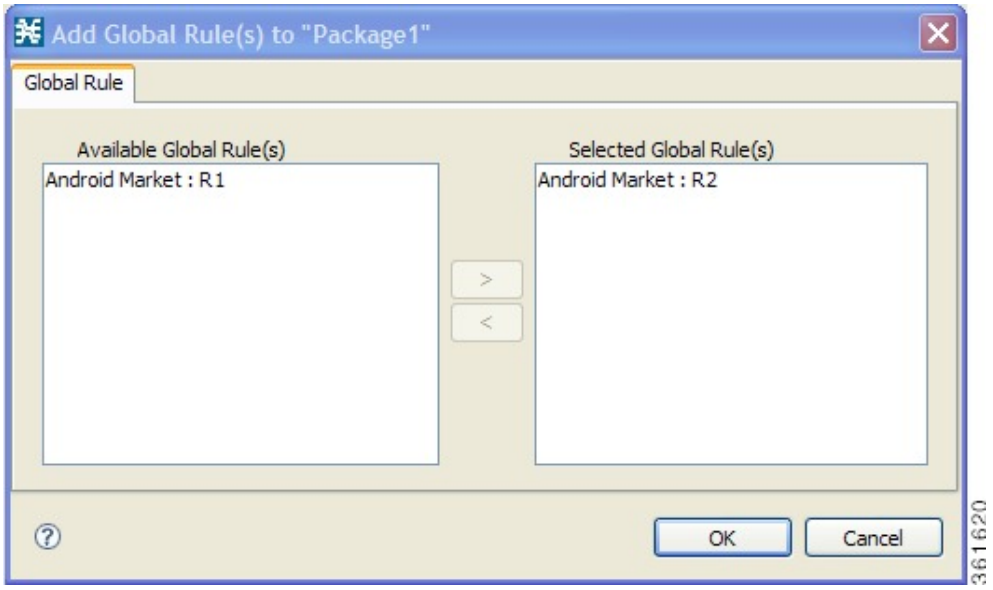
Procedure

Step 1 In the Policies tab, click a package from the package tree.

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

The Add New Global rules to package dialog box appears.

Figure 235: Add Global Rule to Package



Step 3 In the Global Rules Available area of the Add New Global rules to package dialog box, click the rule and click the **Add** button.

Note You can add only one global rule that belongs to a service to a package.

Step 4 Click **OK**.

The Add New Global rules to package dialog box closes.

The service rule is applied to the package.

What to Do Next

Usage limits and breach handling are part of quota management (see “Managing Quotas” section):

- To configure parameters in the Usage Limits tab, see the Selecting Quota Buckets for Rules section.
- To configure parameters in the Breach Handling tab, see the Editing Breach-Handling Parameters for a Rule section.

Deleting a Global Rule from a Package

You can delete a global rule from a package. If you delete a global rule from a package, the global rule is deleted only from the specific package and not from other packages.

To delete a global rule from a package, perform these steps:

Procedure

Step 1 In the Policies tab, click the package from which you want to delete a global rule.

Step 2 In the right (Rule) pane, click a rule to delete.

Step 3 Click the **Delete Rule** icon.
A Rule Warning message appears.

Step 4 Click **Yes**.
The selected rule is deleted from the package.

Displaying Packages Associated to a Global Rule

You can view all the packages associated to a global rule. To view the services affected by any global rule, perform these steps:

Procedure

Step 1 In the Policies tab, click **Global Rule**.

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

Step 3 In the Rule pane, click the **Show All Packages Associated With This Rule** icon.

A Packages Associated with a Global Rule dialog box appears.

Figure 236: Packages Associated with a Global Rule



Step 4 Click **OK** to close the dialog box.

Time-Based Rules Overview

The Console allows you to divide the week into four time frames (see “Managing Calendars” section). A time-based rule is a rule that applies to one time frame.

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

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

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

Adding Time-Based Rules to a Rule

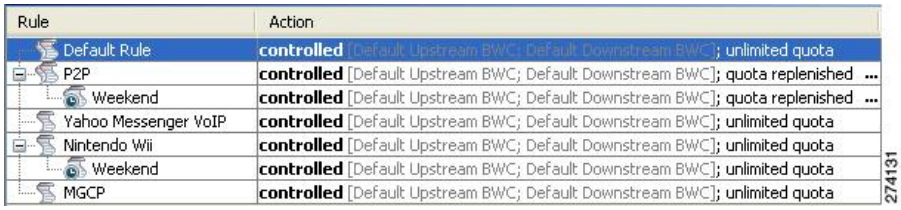
Adding a time-based rule to a rule allows you to specify alternate rule parameters applicable only for a specific time frame. If a time-based rule is not defined for a time frame, the parent rule is enforced.

- When you add a time-based rule, all parameters are initially set to the values defined for the parent rule. Subsequent changes to the parent rule do not change the time-base rule.

- The tabs of the Add New Time-Based Rule dialog box are the same as the tabs of the Add New Rule to Package dialog box, except for the General tab. In the Add New Rule to Package dialog box, you select a service; in the Add New Time-Based Rule dialog box, you select a time frame.

A service whose time-based rule affects any of its child services is indicated in the rules list by a modified icon

Figure 237: P2P Weekend Based Time Rule



Procedure

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

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

Step 3 Click the Add Time-Based Rule icon.
The Add New Time-Based Rule dialog box appears.

Step 4 In the Time Frame area, from the Select the Time Frame for this Rule drop-down list, select one of the four time frames.

Step 5 In the Rule State area, select one of the **Define the State of this Rule** radio buttons.

- Enable reporting and active actions
- Disable reporting and active actions

Step 6 Define behavior per traffic flow.

Step 7 Click the **Control** tab.
The Control tab opens.

Step 8 Follow the instructions in How to Define Per-Flow Actions for a Rule.

Step 9 Change usage limits.

Step 10 Click the **Usage Limits** tab.
The Usage Limits tab opens.

Step 11 Follow the instructions in How to Select Quota Buckets for Rules.

Step 12 Define behavior when a quota is breached.

Step 13 Click the Breach Handling tab.
The Breach Handling tab opens.

Step 14 Follow the instructions in How to Edit Breach-Handling Parameters for a Rule.

Step 15 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.

Editing Time-Based Rules

You can edit time-based rules.

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

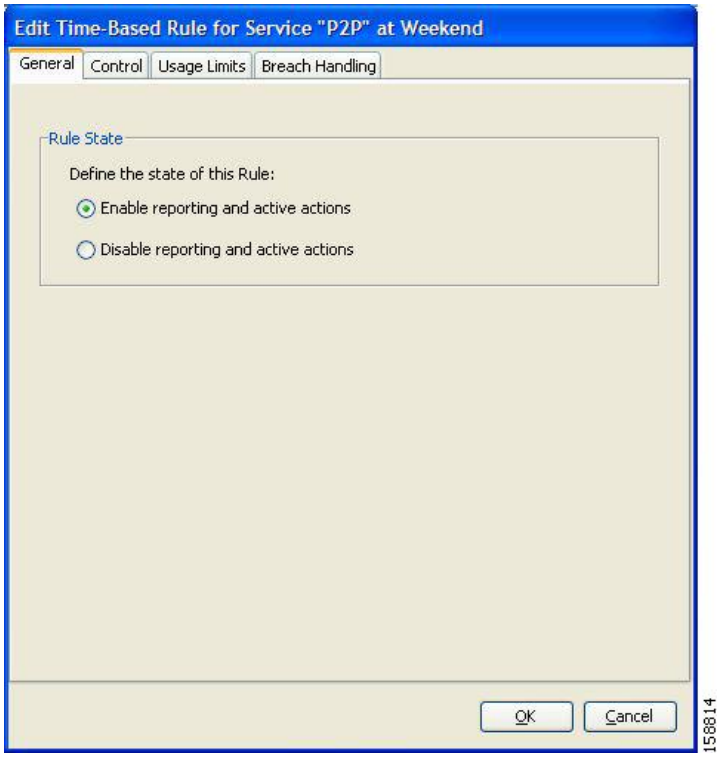
Procedure

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

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

Step 3 Click the Edit Rule icon.
The Edit Time-Based Rule for Service dialog box appears.

Figure 238: Edit Time-Based Rule for Service



Step 4 In the Rule State area, select one of the Define the State of this Rule radio buttons.

- Enable reporting and active actions
- Disable reporting and active actions

Step 5 Define behavior per traffic flow.

Step 6 Click the Control tab.
The Control tab opens.

Step 7 Follow the instructions in How to Define Per-Flow Actions for a Rule.

Step 8 Change usage limits.

Step 9 Click the Usage Limits tab.
The Usage Limits tab opens.

Step 10 Follow the instructions in How to Select Quota Buckets for Rules.

Step 11 Define behavior when a quota is breached.

Step 12 Click the Breach Handling tab.
The Breach Handling tab opens.

Step 13 Follow the instructions in How to Edit Breach-Handling Parameters for a Rule.

Step 14 Click OK.
The Edit Time-Based Rule for Service dialog box closes.

All changes to the time-based rule are saved.

Deleting Time-Based Rules

You can delete any time-based rule.



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

Procedure

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

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

Step 3 In the Rule pane, click the Delete Rule icon.
A Rule Warning message appears.

Step 4 Click Yes.
The selected rule is deleted.

Managing Calendars Overview

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

After you have configured a calendar, you can add time-based rules to a package that uses the calendar. A time-based rule is a rule that applies to only one time frame. Time-based rules allow you to set rule parameters that apply only at specific times. You might, for example, want to define different rules for peak, off-peak, nighttime, and weekend usage.

Each service configuration includes one default calendar. You can add nine more calendars, each with a different time-frame configuration. You can use different calendars for different packages. You can also use different calendars where a service provider has customers in more than one time zone by configuring calendars with a one-hour offset from each other.

- How to View Calendars
- How to Add Calendars
- How to Rename the Time Frames
- How to Delete Calendars
- How to Configure the Time Frames

Adding Calendars

Each service configuration includes one default calendar. You can add up to nine more calendars.

Procedure

Step 1 From the Policies tab of the left pane, choose Configuration > Policies > Weekly Calendars.
The Calendar Settings dialog box appears.

Step 2 In the Calendar tab, click the Add (158725.jpg) icon.
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.

Figure 239: Calendar Parameters Tab



Step 4 Click Close.
The Calendar Settings dialog box closes, and the new calendar name is 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 you can configure the time frames differently in each calendar, the names of the time frames are the same in all of the calendars. If you change the name when configuring one calendar, the names are also changed for all other calendars.

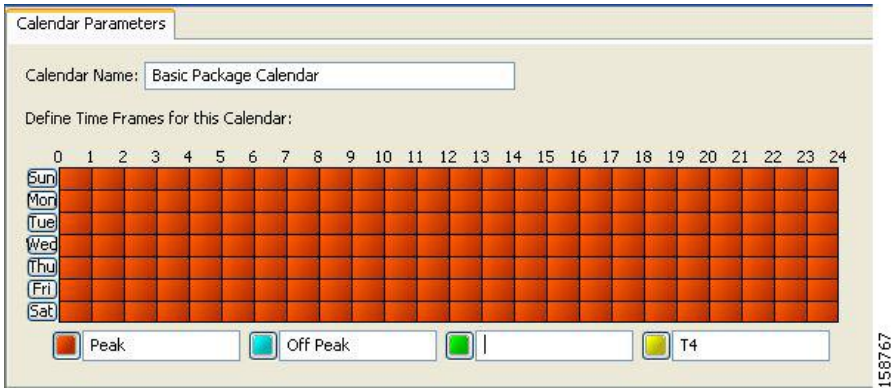
Procedure

Step 1 From the Policies tab of the left pane, choose Configuration > Policies > Weekly Calendars .
The Calendar Settings dialog box appears.

In the Calendar Parameters tab, below the grid, each of the four time frames is listed in a field next to a colored square.

Step 2 Click in a Time Frame Name field, and enter a new name for the time frame.

Figure 240: Calendar Parameters Tab



Step 3 Repeat Step 2 for the other three time frames.

Step 4 Click Close.
The Calendar Settings dialog box closes, and the changes to the names of the time frames are saved.

Viewing Calendars

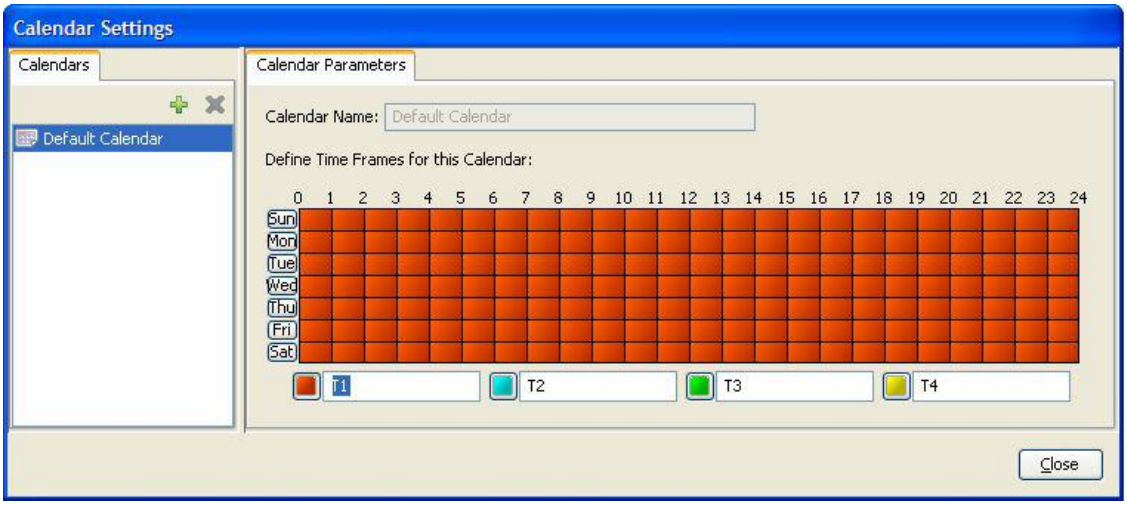
You can view a list of existing calendars and their time frames.

Procedure

Step 1 From the Policies tab of the left pane, choose Configuration > Policies > Weekly Calendars .

The Calendar Settings dialog box appears with a list of existing calendars.

Figure 241: Calendar Settings



Step 2 Click a calendar in the list to display its time-frame settings.
The time frames for the selected calendar are displayed and configured in the Calendar Parameters tab.

Step 3 Click Close.
The Calendar Settings dialog box closes.

Deleting Calendars

You can delete any user-added calendar. The default calendar cannot be deleted.

Note A calendar used by a package cannot be deleted. (When you select the calendar, the Delete icon is dimmed.) To delete the calendar, you must first select a different calendar for each package using the calendar that is deleted. See “How to Set Advanced Package Options” section for information about changing the calendar associated with a package.

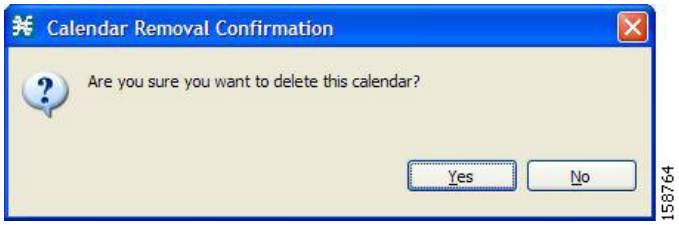
Procedure

Step 1 From the Policies tab of the left pane, choose **Configuration** > **Policies** > **Weekly Calendars**.
The Calendar Settings dialog box appears.

Step 2 In the Calendar tab, select a calendar and click the Delete icon.

A Calendar Removal Confirmation message appears.

Figure 242: Calendar Removal Confirmation



Step 3 Click Yes .
The calendar is deleted.

Step 4 Click Close.

Configuring the Time Frames

By default, all the hours of the week belong to one time frame. The Console allows you to assign each of the 168 (24x7) hours of the week to one of four separate time frames. These time frames allow you to supply time-dependent differentiated services and to impose constraints on any service.

You might want, for example, to divide the week as follows:

- Peak
- Off Peak
- Night
- Weekend

You can define different time frames for each calendar.

Procedure

Step 1 From the Policies tab of the left pane, choose **Configuration** > **Policies** > **Weekly Calendars**.
The Calendar Settings dialog box appears.

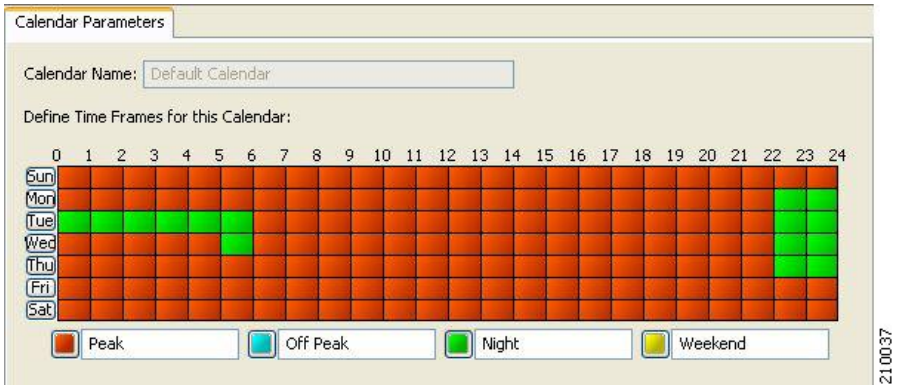
Step 2 In the Calendars tab, select a calendar to configure.
In the Calendar Parameters tab, the selected calendar's Define Time Frames for this Calendar grid is displayed. The grid, representing one week, is laid out in a format of 24 hours x 7 days. Each cell represents one hour.

Below the grid, the name of each time frame appears next to a colored button.

Step 3 Click one of the colored buttons.

Step 4 Select all the cells in the grid that represent hours that are part of the selected time frame.
You can select a group of cells by holding down the mouse button and dragging across the cells.

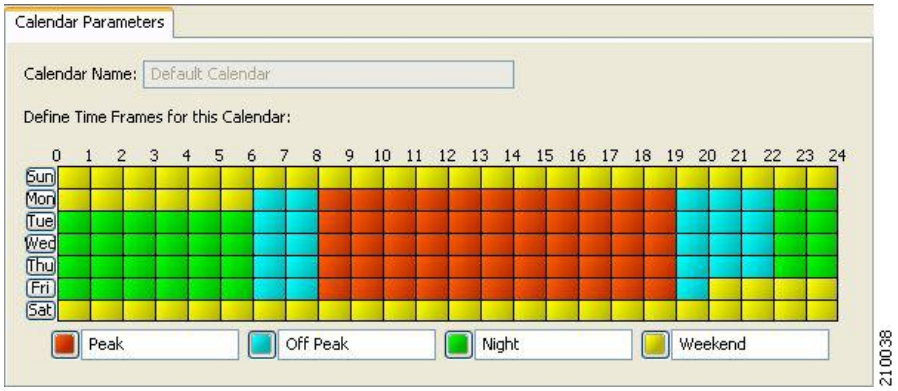
Figure 243: Calendar Parameters Tab



The changes are written to the service configuration as you make them.

Step 5 Repeat Steps 3 and 4 for the other time frames until you have mapped the entire grid.
You have now mapped the week into four different time frames.

Figure 244: Time Partition Plan Example



Step 6 Click Close.
The Calendar Settings dialog box closes.

How to Manage DSCP ToS Marker Values

Cisco SCA BB can change the value of the DSCP ToS marker of packets of flows that match a filter rule or a service rule.

For details on how to change the value of the DSCP ToS marker, see the following steps:

- For Filter Rule—see Step 11 of "How to Add Filter Rules" section
- For Service Rule—see Steps 10 and 11 of "How to Define Per-Flow Actions for a Rule" section and Step 9 of "How to Edit Breach-Handling Parameters for a Rule" section

Cisco SCA BB supports seven ToS Marker Classes. You assign each class a specific value to apply to the packets of a flow.

Note If you have used DSCP marking on a Cisco SCA BB release before 3.1.5 and you are converting your old service configurations, you must reconfigure the service configurations to obtain the same network behavior as in the former release.

Configuring DSCP ToS Marking

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

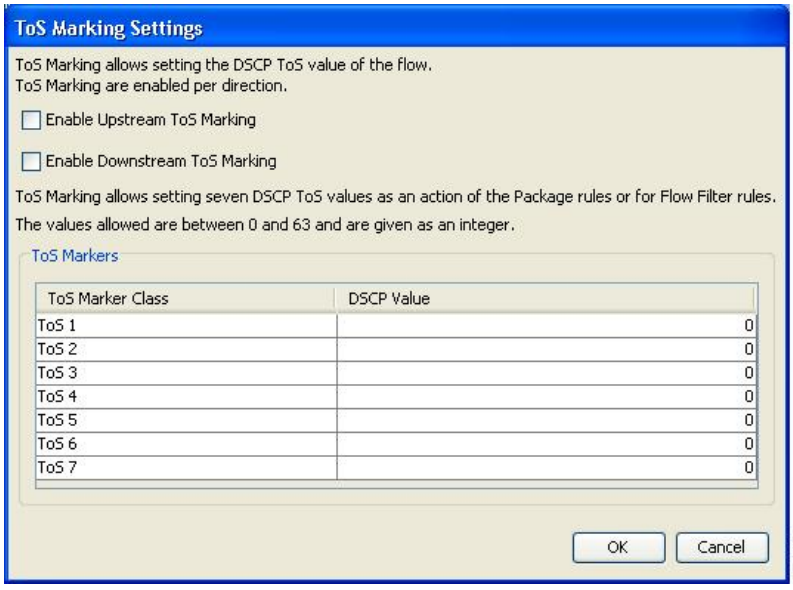
The default marking option is not to mark the packet. The classification may take a few packets to finalize. So after the ToS marking is enabled, the first few packets may still be processed under the default option and therefore may not be marked.

Note In an MPLS environment, the Cisco SCE platform does not map the DSCP bits to the EXP bits of the MPLS header.

Procedure

Step 1 From the Policies tab of the left pane, choose Configuration > Policies > ToS Marking Settings .
The ToS Marking Settings dialog box appears.

Figure 245: ToS Marking Settings



Step 2 (Optional) To enable DSCP ToS marking on upstream flows, check the Enable Upstream ToS Marking check box.

If Upstream ToS Marking is disabled, it overrides filter rule and service rule settings.

Step 3 (Optional) To enable DSCP ToS marking on downstream flows, check the Enable Downstream ToS Marking check box.
If Downstream ToS Marking is disabled, it overrides filter rule and service rule settings.

Step 4 Give unique names to the ToS Marker Classes.

Note You can use the default names for the ToS Marker Classes, but it is recommended that you provide meaningful names.

Step 5 Assign values to the ToS Marker Classes.
Values must be in the range from 0 to 63.

Note When defining filter rules and service rules, the names and values of ToS Marker Classes are displayed in drop-down lists in the format “name [value]”. For example, “ToS 1 [23]” or “My P2P ToS [1]”

Step 6 Click OK .
Your changes are saved.

The ToS Marking Settings dialog box closes.

Quota Management

Related Topics

Global Bandwidth Control , on page 31

Adding Quota Profiles

You can add and define new profiles and edit existing profiles. Additionally, you can add up to 16 new buckets.

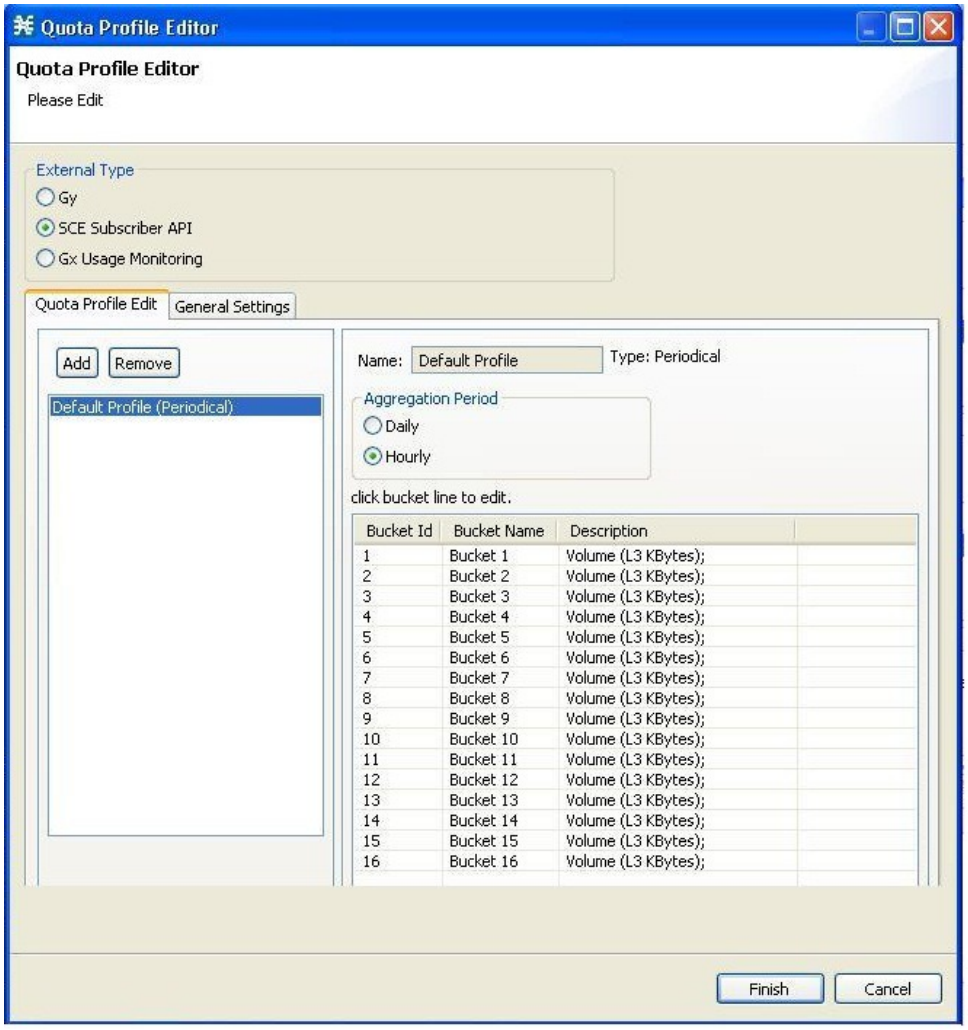
You also define the quota buckets associated with the package. Rules can use quota buckets to set limits to the consumption of particular service groups (see “How to Select Quota Buckets for Rules” section).

Procedure

Step 1 From the Policies tab in the left pane, choose Configuration > Policies > Quota Settings.

The Quota Profile Editor dialog box appears.

Figure 246: Quota Profile Editor



Step 2 Select one of the External Type radio buttons.

- Gy—The Gy quota model enables the Gy interface adapter to be used for the external quota management. For more information, see the Cisco Service Control Mobile Solution Guide.
- SCE Subscriber API—The Subscriber API enables the external applications (policy servers) to connect directly to the Cisco SCE for subscriber provisioning. For more information, see the Cisco Service Control SCE Subscriber API Programmer Guide.
- Gx Usage Monitoring—Gx Usage Monitoring enables the Gx interface to generate usage monitoring reports. For more information, see the Cisco Service Control Mobile Solution Guide.

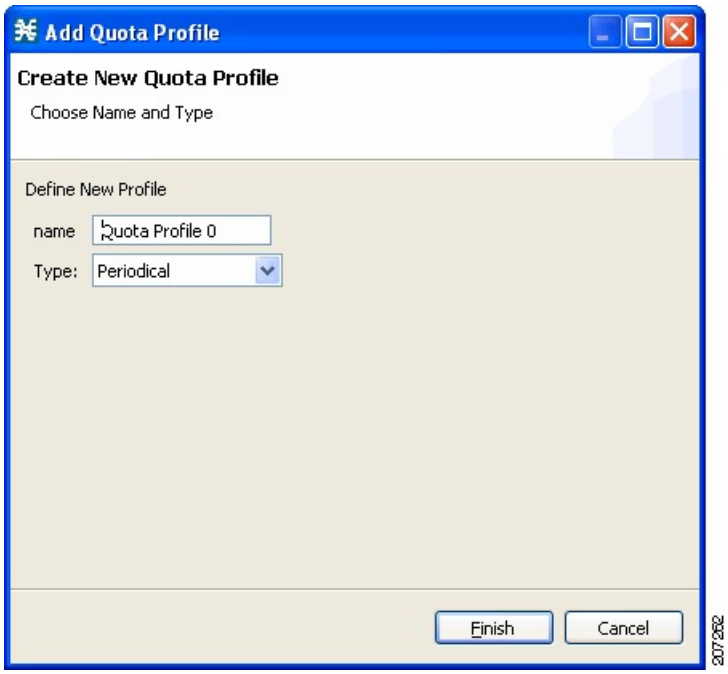
Note Using periodical quota management, you can scatter quota replenishment so that the quota of all subscribers is not replenished at the same time. (See “Quota Replenish Scatter” section.)

Step 3 For Periodical quota profile, select one of the Aggregation Period radio buttons to specify when the quota is renewed for the package:

- Hourly—Replenishes quota at each hour change
- Daily—Replenishes quota at midnight

Step 4 In the Quota Profile Edit tab, click Add.
The Add Quota Profile dialog box appears.

Figure 247: Add Quota Profile



Step 5 In the Name field, enter a unique name for the new quota profile.

Step 6 Select the Type from the drop-down list.

- Periodical
- Subscriber SCE API

Step 7 Click Finish.
The Add Quota Profile window closes.

The new profile is added to the list of profiles displayed in the left (Quota Profile Edit) pane.

Editing Quota Profiles

You can edit the profiles to update the bucket profile.



Note You cannot edit or remove the default profile.

Procedure

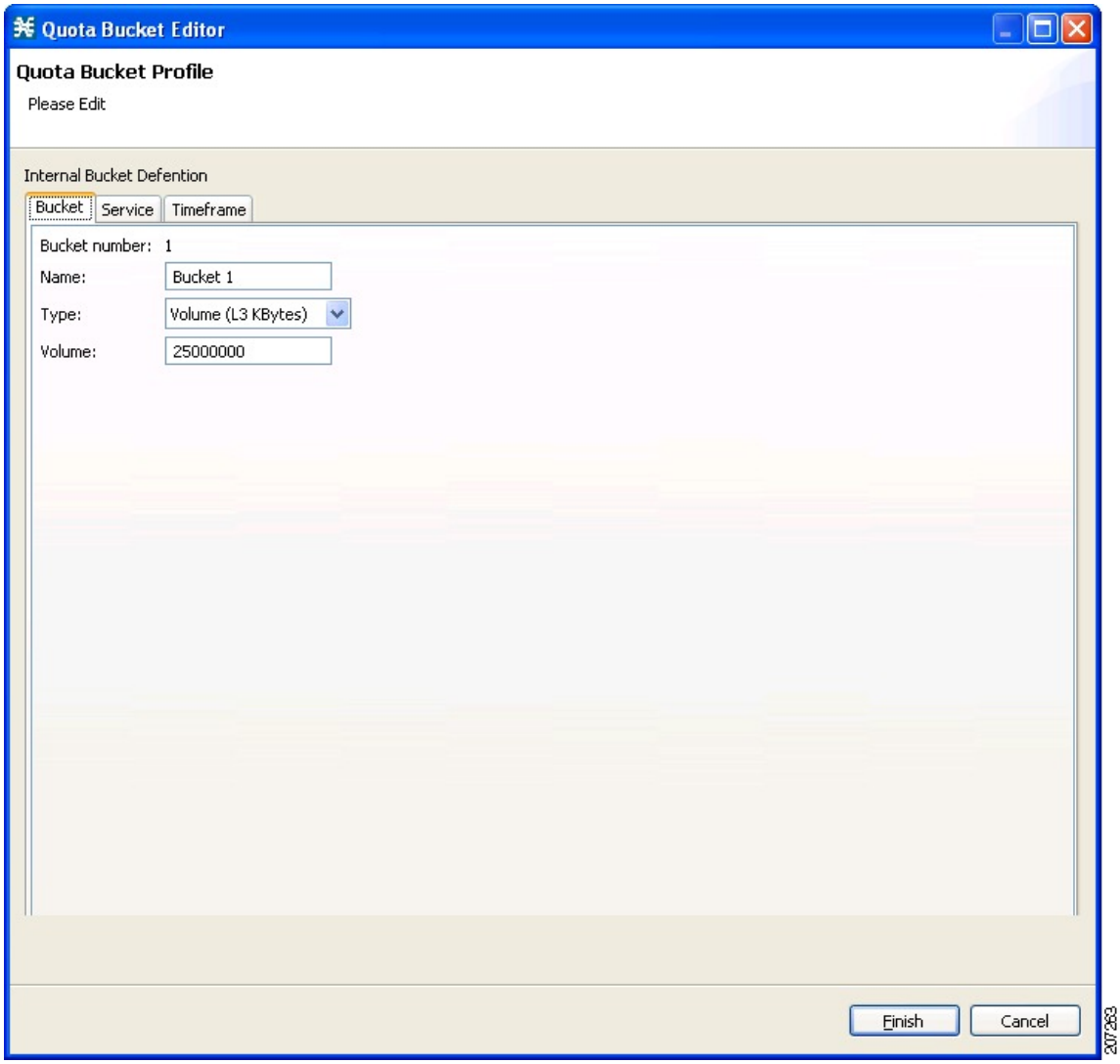
Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies** > **Quota Settings**.
The Quota Profile Editor dialog box appears.

Step 2 Select a quota profile from the profile tree.
All the buckets defined for the selected profile are listed on the right pane.

Step 3 Double-click a bucket line in the right pane.

The Quota Bucket Editor window appears.

Figure 248: Quota Bucket Editor

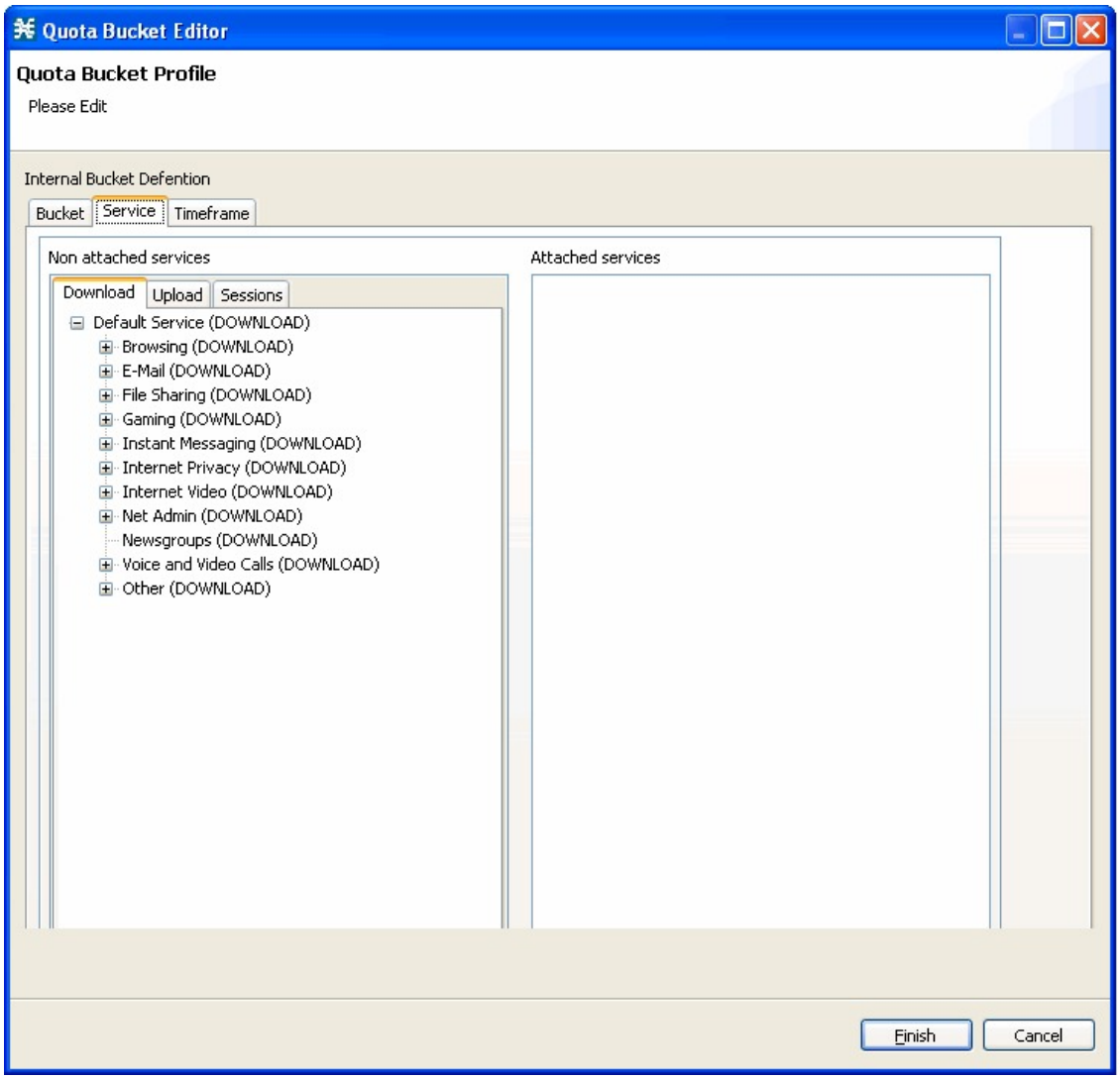


Step 4 Change the Name, Type, and Volume.

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

Step 5 Click on the Service tab, to associate the services to the quota profile.

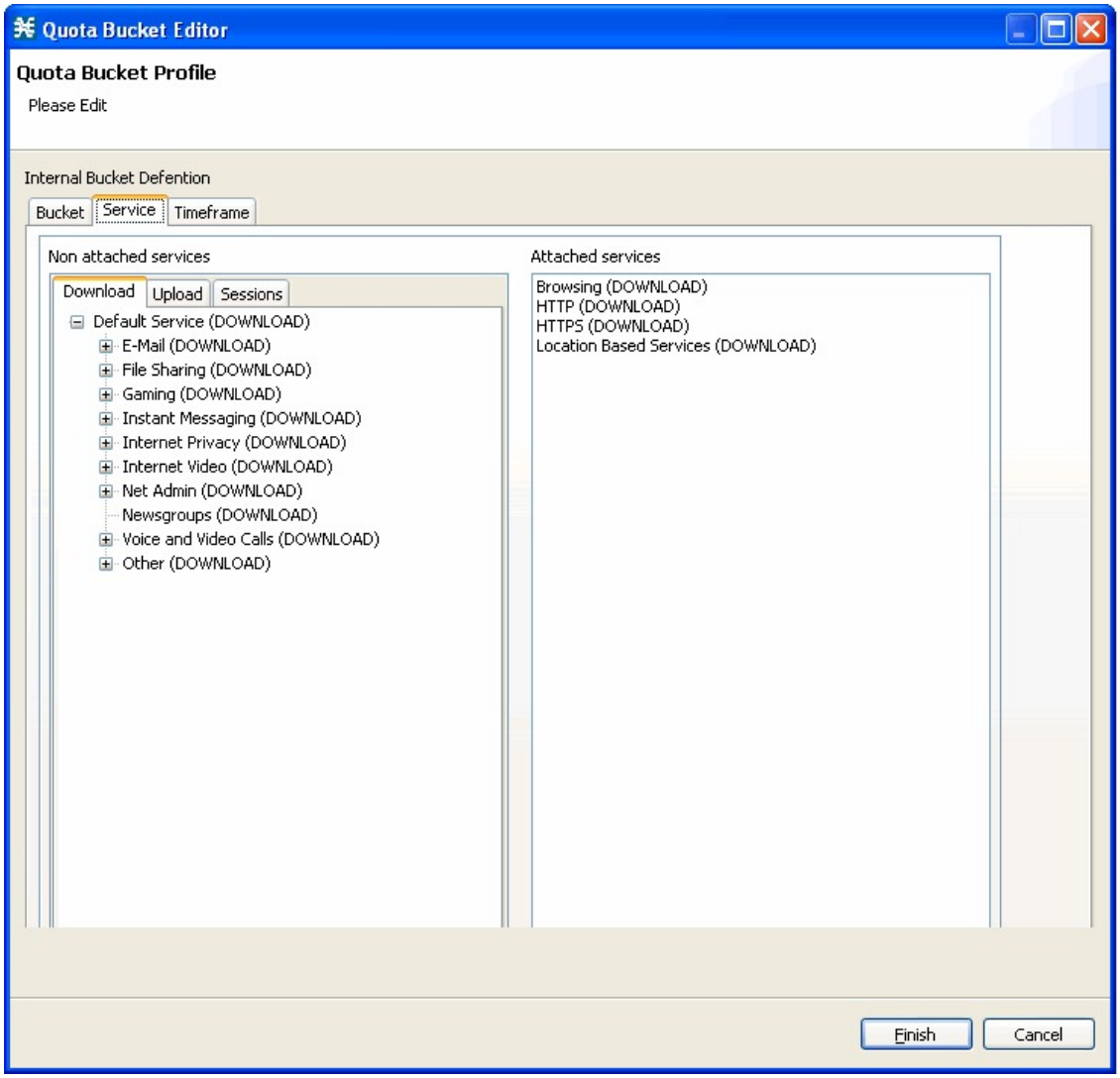
Figure 249: Quota Bucket Editor - Service



Step 6 Select a service from the Non Attached Service pane and move it to the Attached Service pane on the right.

The selected service is moved along with its sub services.

Figure 250: Quota Bucket Editor - Attached Service

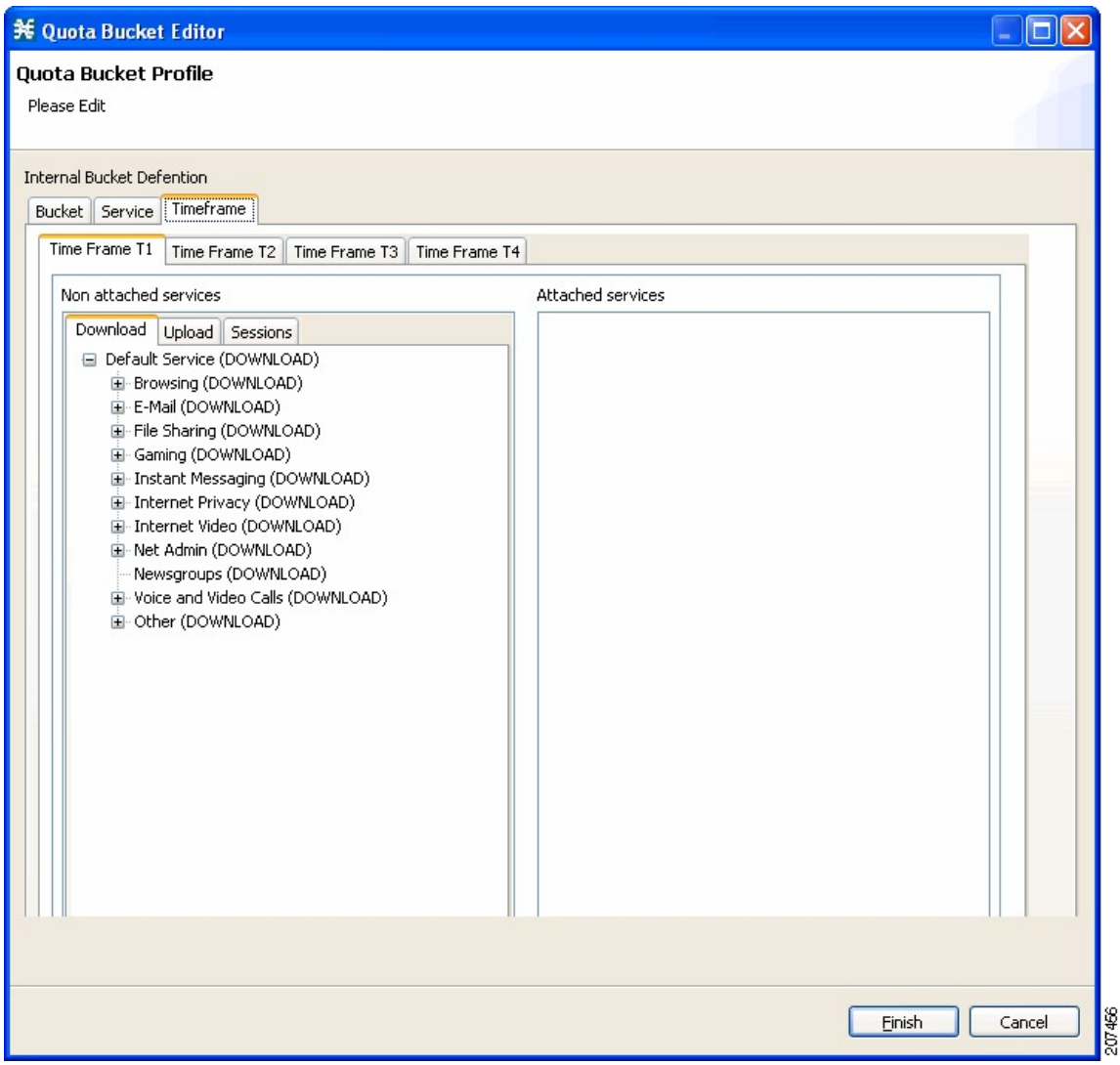


Step 7 Based on the bucket type, you can select services from the following tabs:

- Download
- Upload
- Session

Step 8 Click on the **Timeframe** tab, to associate different timeframes to the quota profile.

Figure 251: Quota Bucket Editor - Timeframe



Step 9 Select a service from the Non Attached Service pane and move it to the Attached Service pane on the right. The selected service is moved along with its sub services.

Step 10 Based on the bucket type, you can select services from the following tabs:

- Download
- Upload
- Session

Step 11 Click **Finish**.
The Quota Bucket Editor closes.

Step 12 Click **Finish**.

The Quota Profile Editor closes.

What to Do Next

To select a service to which the rule relates to, see “How to Add Rules to a Package” section.

Deleting Quota Profiles



Note The default profile cannot be deleted.

Procedure

Step 1 From the Policies tab in the left pane, choose Configuration > Policies > Quota Settings .
The Quota Profile Editor dialog box appears.

Step 2 Select a quota profile from the profile tree.

Step 3 Click Remove.

Step 4 Click Finish.
The Quota Profile Editor dialog box closes.

Editing Quota Management Settings for Packages

You can define whether an external quota manager or the Cisco SCA BB performs the quota management for a package.

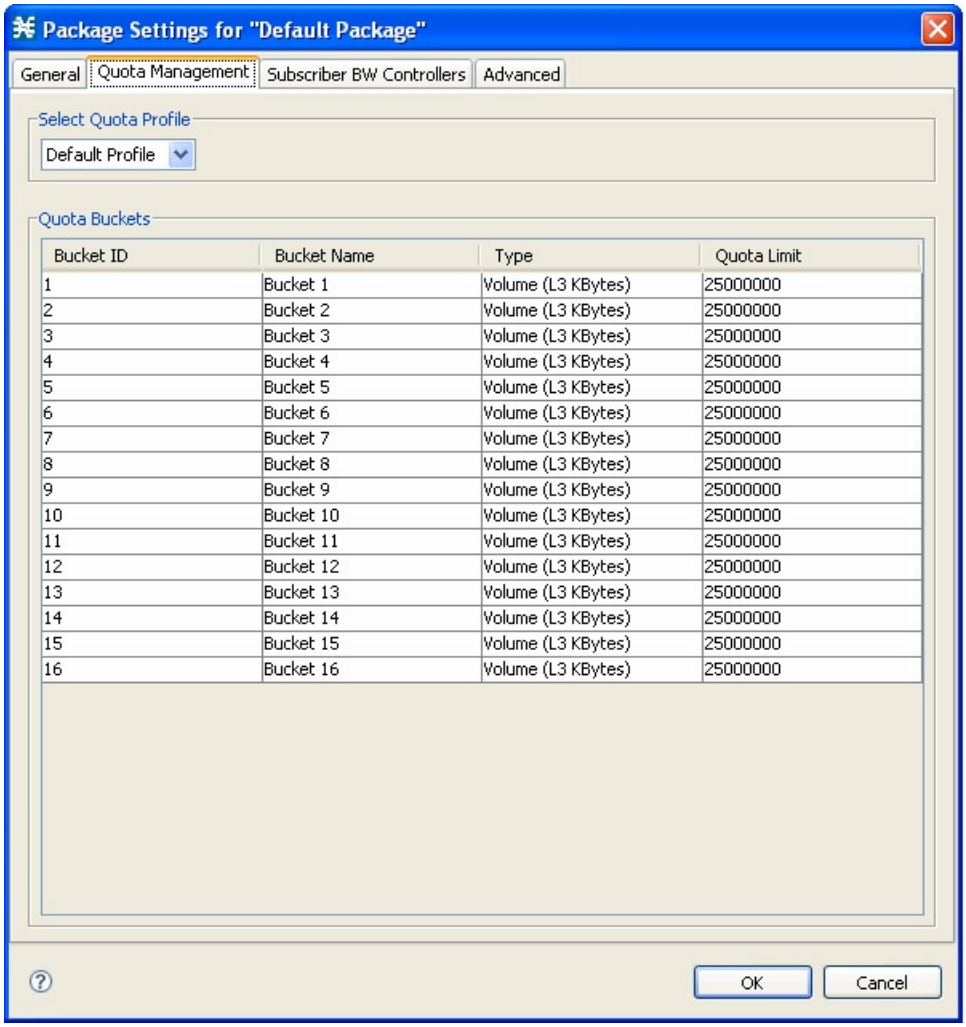
Procedure

Step 1 In the Policies tab, select a package from the package tree, and click the Edit Package icon.
The Package Settings dialog box appears.

Step 2 In the Package Settings dialog box, click the Quota Management tab.

The Quota Management tab opens.

Figure 252: Quota Management Tab



Step 3 Select the Select quota profile from the drop-down list.

Step 4 Click **OK**.
The Package Settings dialog box closes.

All changes to the quota management settings are saved.

Quota Replenish Scatter

By default, if subscriber quota is replenished using periodical quota management, the quota of all subscribers is replenished at the same time. To smooth quota replenishment, you can scatter the time of quota replenishment.

To activate this feature, enter a non-zero value for the Length of the time frame for quota replenish scatter (minutes) property of the Advanced Options tab of the Systems Settings dialog box (see "Managing Advanced Service Configuration Options" section). By default, this property has a value of zero, that is, all quota is replenished at the same time.

Quota for each subscriber is replenished at a random time within the quota replenish scatter time frame, with replenish events split evenly before and after the quota aggregation time.

Best results are obtained if the scatter time frame is the same length as the quota aggregation period, which should completely smooth replenish events. Do not enter a value larger than the quota replenish period. Therefore, for an hourly quota replenish period, set the scatter to 60 minutes.

The quota replenish scatter function is independent of all other quota management parameters.

Selecting Quota Buckets for Rules

Select the quota buckets that the flows mapped to a rule uses. The quota buckets are defined during package setup (see "How to Edit Quota Management Settings for Packages" section). If no quota bucket is appropriate for the rule, add a new quota bucket to the package or edit an existing bucket.

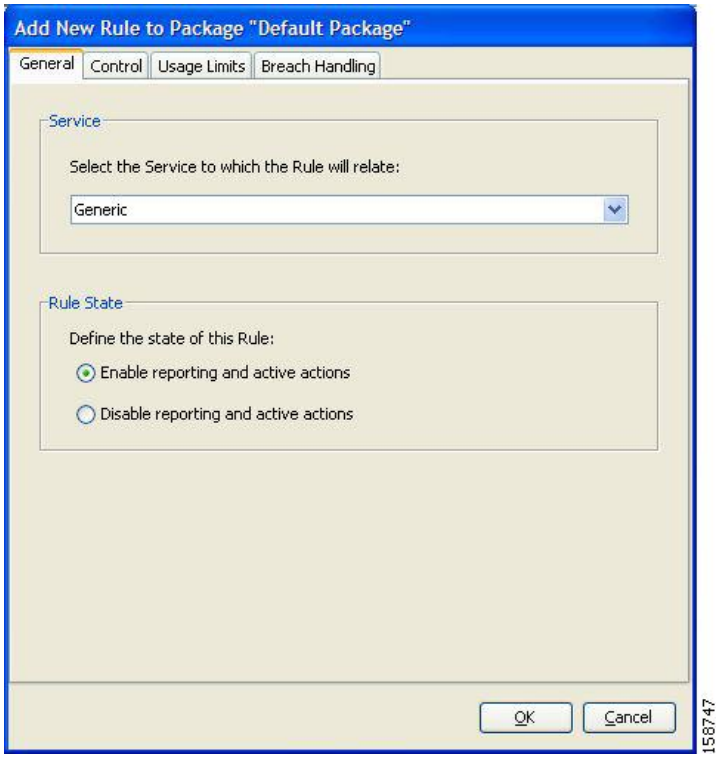
Procedure

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

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

The Add New Rule to Package dialog box appears.

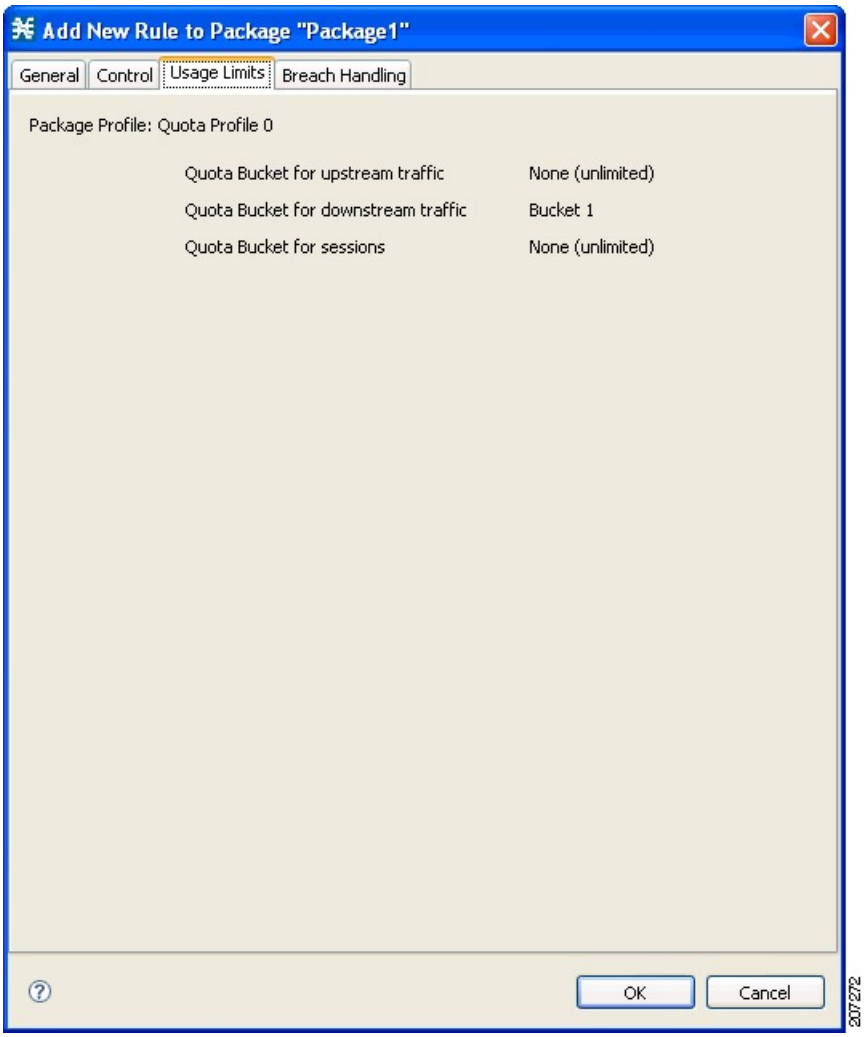
Figure 253: Add New Rule to Package



Step 3 In the Service area, select a service from the Select the Service to Which the Rule Relates drop-down list.

Step 4 Click the Usage Limits tab.

Figure 254: Usage Limits Tab



Step 5 The Usage Limits tab displays the package profile details.
The quota bucket selected for the rule is displayed. For more information on adding services to quota profile, see Step 5 of the “How to Edit Quota Profiles” section.

Step 6 Click OK .
The Edit Rule for Services dialog box closes.

Editing Breach-Handling Parameters for a Rule

You can define the Cisco 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.

Procedure

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

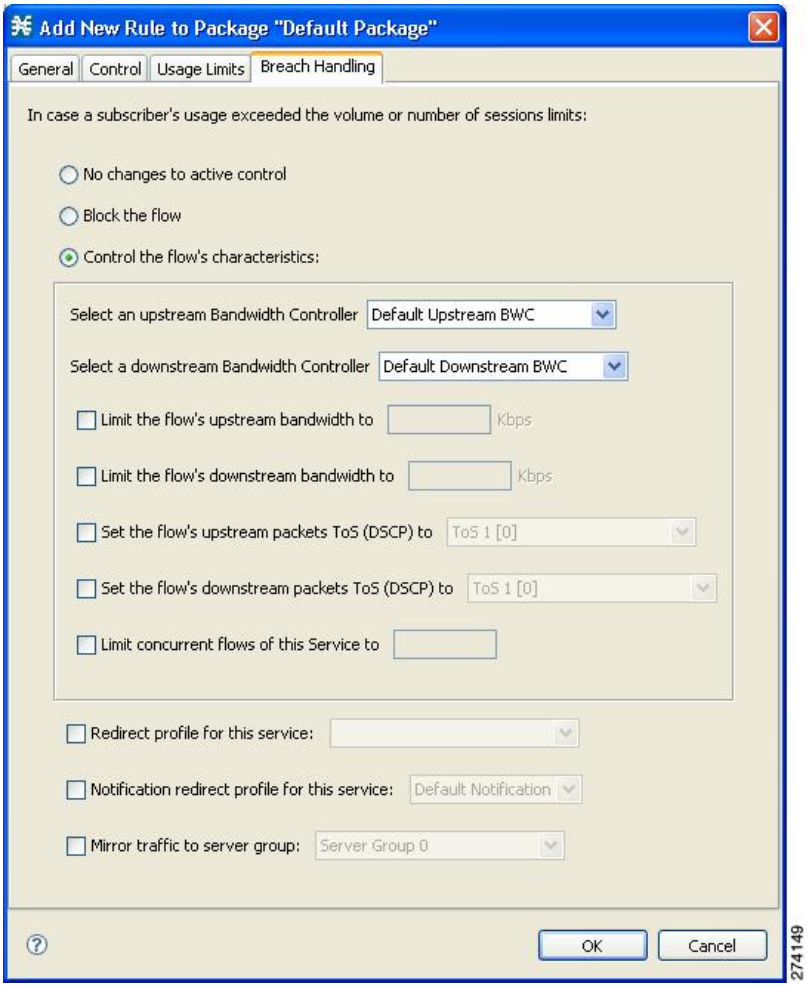
Step 2 In the right (Rule) pane, select a rule.

Step 3 Click the **Edit Rule** icon.
The Edit Rule for Service dialog box appears.

Step 4 Click the Breach Handling tab.

The Breach Handling tab opens.

Figure 255: Breach Handling Tab



Step 5 Set the behavior of the flow when quota is breached.

- To block the flow when quota is breached, continue at Step 6 .
- To change the characteristics of the flow when quota is breached, continue at Step 10 .
- To leave the flow unchanged when quota is breached, select the **No changes to active control** radio button and continue at Step 11 .

Step 6 To block the flow, select the **Block the flow** radio button.

Step 7 Continue at Step 10

Step 8 Change the characteristics of the flow.

a) Select the **Control the flow's characteristics** radio button.
The options in the Flow Characteristic area are enabled:

b) From the upstream Bandwidth Controller drop-down list, select an upstream BWC

The BWCs in this drop-down list are defined when creating or editing the package.

When the mouse is placed over the drop-down list, a tooltip appears. The tooltip contains the properties of the selected BWC, such as PIR, CIR, AL, and Global Controller.

c) From the downstream Bandwidth Controller drop-down list, select a downstream BWC.
d) (Optional) Check the **Limit the flow's upstream bandwidth** check box and enter a value in the Kbps field.
e) Check the **Limit the flow's downstream bandwidth** check box and enter a value in the Kbps field.
f) (Optional) Check the **Set the flow's upstream packets ToS (DSCP) to** check box and select a value from the drop-down list.
g) (Optional) Check the **Set the flow's downstream packets ToS (DSCP) to** check box and select a value from the drop-down list.
h) (Optional) Check the Limit concurrent flows of this Service check box and enter a value in the associated field.

Step 9 (Optional) To enable subscriber redirect, check the check box, and select a redirect profile from the drop-down list.

Step 10 (Optional) To enable subscriber notification, check the Notification redirect profile for this service check box and select a notification redirect profile from the drop-down list.

Note A subscriber notification can be activated in addition to any of the three breach-handling options.

Note Subscriber notification is not supported when unidirectional classification is enabled. If you try to check the Activate a Subscriber Notification check box when unidirectional classification is enabled, a Rule Error message appears.

Step 11 Click OK to continue.

Step 12 (Optional) To enable mirror traffic to a server group, check Mirror traffic to server group and choose a server group to send the mirror traffic to.

Note The Mirror traffic to server group check box is only enabled when Traffic Mirroring is enabled in the VAS Settings dialog box.

Step 13 Click **OK**.
The Edit Rule for Service dialog box closes.

All changes to the rule are saved.

Breach-Handling Parameters

The following are the configuration parameters in the Breach Handling tab of the Edit Rule for Service Settings dialog box.

- You determine what happens to flows identified as belonging to this rule when a quota is breached:
  - No changes to active control—Flows mapped to this rule are not affected when quota is breached. Cisco SCA BB can generate Quota Breach RDRs even when this option is selected (see “How to Manage Quota RDRs” section).
  - Block the flow—Flows mapped to this rule are blocked when quota is breached.

Redirect to—Redirect the flow to a specified, protocol-dependent URL, where a posted web page explains the reason for the redirection. URL redirection sets are defined in the System Settings dialog box. (See “How

to Add a Set of Redirection URLs" section.) Only three protocol types support redirection: HTTP, HTTP Streaming, and RTSP. Redirection is not supported when unidirectional classification is enabled.

- Control the flow characteristics—The behaviors of flows mapped to this rule change when quota is breached:

Select an upstream Bandwidth Controller—Map the traffic flow of this rule to a specific upstream BW controller (BWC). This sets up bandwidth metering of all concurrent flows mapped to this rule, based on the characteristics of the selected BWC.

Select a downstream Bandwidth Controller—The same functionality as the previous option, but for downstream flow.

Limit the flow's upstream bandwidth—Set a per-flow upstream bandwidth limit (for flows mapped to the service of this rule).

Limit the flow's downstream bandwidth—Set a per-flow downstream bandwidth limit.

Set the flow's upstream packets ToS—Set the DSCP ToS marker of all packets of upstream flows.

Set the flow's downstream packets ToS—Set the DSCP ToS marker of all packets of downstream flows.

Limit concurrent flows of this Service—Set the maximum number of concurrent flows (mapped to this rule) permitted to a subscriber.

- Activate a Subscriber Redirect—Activate a Subscriber Redirect when subscribers exceed their quota limit.
- Activate a Subscriber Notification—Activate a Subscriber Notification when subscribers exceed their quota limit. This notification can, for example, convey the quota breach situation to the subscriber and explain how to obtain additional quota.



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

To define Subscriber Notifications, see "Managing Subscriber Notifications" section.

- Activate Traffic Mirroring—Activate traffic mirroring when subscribers exceed their quota limit

Example for Creating Tiered Subscriber Services

Tiered subscriber services can be implemented using the Cisco SCA BB Console. Because the definition of such services is open ended, this section describes how to define two of the tiers outlined in the value proposition description. The two tiers are defined as follows:

- Silver
  - Weekly bandwidth limited to 4.2 GB (corresponds to a daily limit of 600 MB)
  - Email and browsing services are limited to 256 kbps
  - Audio and video streaming services are limited to 64 kbps
  - P2P services are limited to 28 kbps
- Gold

- Weekly bandwidth limited to 5.6 GB (corresponds to a daily limit of 800 MB)
- Email and browsing services are not bandwidth limited
- Audio and video streaming services are limited to 128 kbps
- P2P services are limited to 28 kbps

The following steps are applicable to both the 'Silver' and 'Gold' packages.

Procedure

Step 1 Create a new package as described in “How to Add Packages” section.

Step 2 Enable periodical (internal) quota management.

Step 3 Set the aggregation period to Daily

Step 4 Set the quota limit to the desired value and give the quota bucket a meaningful name
For further information, see “How to Edit Quota Management Settings for Packages” section.

Step 5 Add the bandwidth controllers for the required services and set the PIR to the desired rate.

Note Each service that is bandwidth limited requires a sub bandwidth controller that is a child of the primary bandwidth controller, not an extra bandwidth controller.

For further information, see “How to Edit Package Subscriber BWCs” section .

Step 6 Add a rule to the package for each bandwidth limited service.
For further information, see “How to Add Rules to a Package” section .

Step 7 Configure the rule to control the characteristics of the flow with the bandwidth controller for the relevant service.
For further information, see “How to Define Per-Flow Actions for a Rule” section .

Step 8 Set the usage limit for the package to use the quota bucket defined in Step 2.
For further information, see the “How to Select Quota Buckets for Rules” section section.

Unknown Subscriber Traffic

Cisco SCE platform processes a traffic flow that does not match any filter rule (see “Filtering the Traffic Flows” section on page 10-23). Cisco SCE platform tries to identify the subscriber responsible for the traffic flow. The platform checks its internal database for a subscriber identified by the IP address or VLAN tag of the traffic flow. If no such subscriber exists, the traffic flow is mapped to the Unknown Subscriber Traffic category.

The Unknown Subscriber Traffic category is included in the tree in the Network Traffic tab but is not part of the package hierarchy. The Unknown Subscriber Traffic category cannot be deleted.



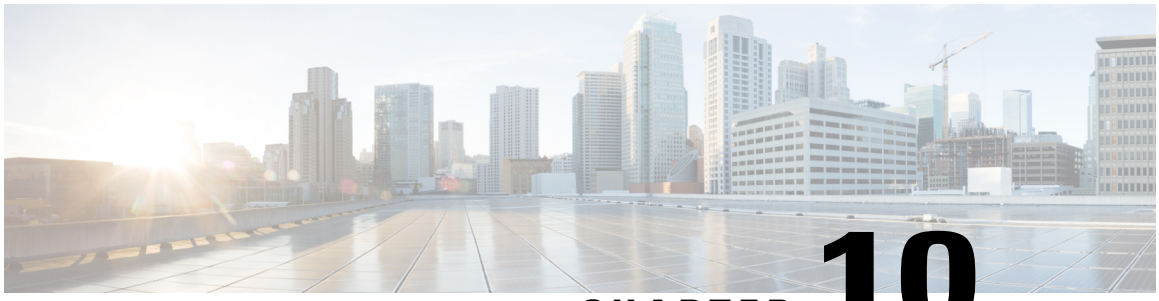
Note Traffic of one unknown subscriber cannot be distinguished from traffic of other unknown subscribers. Therefore, you cannot set either per-subscriber usage limits or subscriber-level metering with subscriber BWCs. You can use subscriber BWCs only to link a selected service to a global controller.

The Unknown Subscriber Traffic category behaves like a package with the following parameters:

- Package Name = Unknown Subscriber Traffic
- Package Index = 4999
- One package usage counter:
  - Counter Name = Unknown Subscriber Traffic Counter
  - Counter Index = 1023

You can:

- Edit the Unknown Subscriber Traffic package settings:
  - Add extra BWCs (see “How to Edit Package Subscriber BWCs” section).
  - Select a calendar (see “How to Set Advanced Package Options” section).
- Edit the default service rule for the Unknown Subscriber Traffic category:
  - Change the Rule State (see “How to Edit Rules” section).
  - Change per-flow actions for the rule (see “How to Define Per-Flow Actions for a Rule” section).
- Add rules to the Unknown Subscriber Traffic package:
  - Add rules (see “How to Add Rules to a Package” section); edit (see “How to Edit Rules” section) and delete (see “How to Delete Rules” section) these rules.
  - Add time-based rules (see “How to Add Time-Based Rules to a Rule” section); edit (see “How to Edit Time-Based Rules” section) and delete (see “How to Delete Time-Based Rules” section) these rules.



CHAPTER 10

Service Configuration Editor: Additional Options

This chapter explains how to use additional, advanced functionality available in the Service Configuration Editor.

This chapter consists of these sections:

- The Service Security Dashboard , page 379
- Traffic Flow Filtering, page 399
- Managing Subscriber Notifications Overview, page 416
- Managing Subscriber Redirection Overview, page 424
- Managing the System Settings Overview, page 433
- Managing VAS Settings Overview, page 444
- Managing the Protected URL Database, page 456

The Service Security Dashboard

The Service Security Dashboard allows you to view and control all Cisco SCA BB security functionality.

The Dashboard is a gateway to a set of features that help you protect your network from security threats such as worms, DDoS attacks, and spam zombies. It allows configuration of the detection mechanisms (for example, attack thresholds) and of the actions to be taken when an attack is detected.

The Dashboard also allows you to access malicious traffic reports in the Reporter tool.

Note If anomaly-based detection of malicious traffic is enabled, any access control list (ACL) that is configured on the Cisco Service Control Engine (Cisco SCE) platform but is not applied to anything (for example, an interface, an access map, or an SNMP community string) might be deleted when a service configuration is applied to the platform. Workaround : Disable anomaly-based detection of malicious traffic. (Clear the Enable anomaly detection check box.)

Viewing the Service Security Dashboard

Procedure

In the Network Traffic tab, select Service Security .
The Service Security Dashboard is displayed in the right pane.

Figure 256: Service Security Dashboard



Introduction to Managing Worm Detection

Cisco SCA BB uses three mechanisms for detecting worms:

- Signature-based detection—The stateful Layer 7 capabilities of the Cisco SCE platform can detect malicious activity that is not easily detectable by other mechanisms. You can add signatures for new worms.
- Anomaly-based detection—Overall traffic analysis can detect anomalies that might indicate worm activity. See Managing Anomaly Detection Overview, on page 381 section.
- Mass-mailing based detection—E-mail traffic analysis can detect anomalies that might indicate e-mail-based worms. See Configuring Spam Detection Settings , on page 395 section.

For more information, see Introduction to Managing Protocol Signatures , on page 200 section.

Viewing Supported Worm Signatures

Procedure

Step 1 In the Service Security Dashboard, click View Signatures .

The Signatures Settings dialog box appears, with Worm Signatures selected in the Signature Type drop-down list.

All supported worm signatures are listed.

Step 2 Click **Close**.
The Signatures Settings dialog box closes.

Adding New Worm Signatures to a Service Configuration

Either import the latest DSS or SPQI file provided by Cisco or create a DSS file containing any worm signatures that you wish to add to the service configuration.

Managing Anomaly Detection Overview

The most comprehensive threat detection method is anomaly detection.

Anomaly Detection

The basic principle of anomaly detection is monitoring successful (correctly established for TCP, bidirectional for other protocols) and unsuccessful (not properly established for TCP, unidirectional for other protocols) connection rates both to and from any IP address viewed by the system, and triggering an anomaly detection condition based of one of the following criteria:

- The total connection rate exceeds a predefined threshold.
- The suspicious connection rate exceeds a predefined threshold and the ratio of suspicious to unsuspicious connections exceeds a predefined threshold.

The ratio metric is a robust indicator of malicious activity, and together with a rate qualifier it serves as a reliable identifier for malicious activity.

Anomaly detection is divided into three categories based on the directional nature of the detected anomaly condition. The concepts used for the three categories are identical, but the nature of the detected malicious activity is different for each category.

- Scan/Sweep detector—Detects malicious activity based on an anomaly in connection rates from an IP address.
- DoS detector—Detects an anomaly in the connection rate between a pair of IP addresses: one of them is attacking the other. This can be either an isolated attack or part of a larger scale DDoS attack.
- DDoS detector—Detects an anomaly in the connection rate coming to an IP address, which means that it is being attacked. The attack can be by either a single IP address (DoS) or multiple IP addresses.



Note When the IP address common to all flows of an attack is on the network side, the Cisco SCE may require more flows (than the configured threshold) to detect the attack.

For all kinds of anomaly detection conditions, maximum flexibility is provided by the ability to define detection thresholds and the trigger actions to be taken for each:

- Flow direction
- Flow protocol
- (Optional) Port uniqueness for TCP and UDP

Note The GUI configuration described here replaces the CLI command set for configuring the Attack Filtering Module of the Cisco SCE platform, which was available in previous releases.

Anomaly Detection Parameters

For each anomaly detector category (Scan/Sweep, DoS, DDoS) there is one default detector. You can add additional detectors of each category. Detectors in each category are checked in order; the first match (according to the threshold settings of the detector) triggers detection. You set the order in which detectors are checked; the default detector is checked last.

Anomaly detectors can contain up to 12 anomaly types associated with malicious traffic:

- Network initiated—Malicious traffic initiated from the network side:
  - TCP—Aggregate TCP traffic on all ports
  - TCP Specific Ports—TCP traffic on any single port
  - UDP—Aggregate UDP traffic on all ports
  - UDP Specific Ports—UDP traffic on any single port
  - ICMP—Aggregate ICMP traffic on all ports
  - Other—Aggregate traffic using other protocol types on all ports
- Subscriber initiated—Malicious traffic initiated from the subscriber side:
  - TCP
  - TCP Specific Ports
  - UDP
  - UDP Specific Ports
  - ICMP
  - Other

Note ICMP and Other anomaly types are not available for DoS attack detectors.

Each anomaly type on a detector has the following attributes associated with it:

- Detection thresholds—There are two thresholds, crossing either of them means that an attack is defined to be in progress:
  - Session Rate threshold—The number of sessions (per second) over specified ports for a single IP address that trigger the anomaly detection condition.
  - Suspected sessions threshold—Suspected sessions are sessions that are not properly established (for TCP), or that are unidirectional sessions (for other protocols). Exceeding both the Suspected Session Rate *and* the Suspected Session Ratio triggers the anomaly detection condition. (A relatively high session rate with a low response rate typically indicates malicious activity.)
  - Suspected Session Rate—The number of suspected sessions (per second) over specified ports for a single IP address.
  - Suspected Session Ratio—The ratio (as a percentage) between the suspected session rate and the total session rate. A high ratio indicates that many sessions received no response, an indication of malicious activity.
- Actions—Zero or more of the following actions may be taken when an anomaly detection condition is triggered (by default, no action is enabled):
  - Alert User—Generate an SNMP trap indicating the beginning and end of an anomaly. For details on SNMP traps, see the "SCA BB Proprietary MIB Reference" chapter of *Cisco Service Control Application for Broadband Reference Guide* for information about the Cisco proprietary MIB.
  - Notify Subscriber—Notify the relevant subscriber of the malicious activity by redirecting the browsing sessions to a captive portal. To configure network attack subscriber notification, see Managing Subscriber Notifications Overview, on page 416 section.
  - Block Attack—Block the relevant sessions. Blocking is performed based on the specification of the malicious traffic that triggered the anomaly detection condition. If subscriber notification is enabled for the anomaly type, blocking is not applied to the port relevant for browsing (by default, this is TCP port 80; see Advanced Service Configuration Options, on page 435 section).



Note Logging of the anomaly to an on-device log file and generation of RDRs is not configurable per anomaly type.

- User-defined detectors can also have one or more of the following attributes:
  - IP address list—Limit detection to the listed IP address ranges. This applies to the source IP when detecting IP sweeps and port scans. It applies to the destination IP when detecting DoS and DDoS attacks.
  - TCP port list—Limit detection to the listed destination TCP ports. This list is applied to TCP Specific Ports anomaly types only.
  - UDP port list—Limit detection to the listed destination UDP ports. This list is applied to UDP Specific Ports anomaly types only.

Viewing Anomaly Detection Settings

You can view a list of all anomaly detectors. The anomaly detectors are displayed in a tree, grouped according to detector category (Scan/Sweep, DoS, or DDoS).

For each anomaly detector, you can view its associated parameters and see a list of all anomaly types included in the detector, together with their parameters.

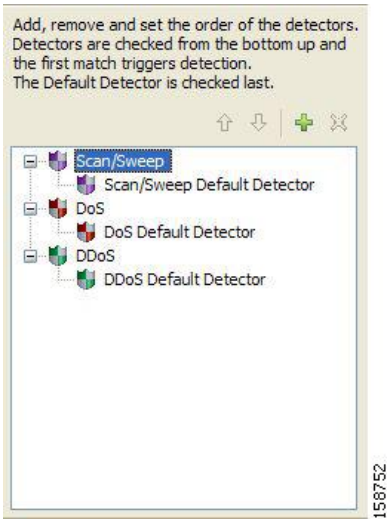
Procedure

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click Configure .

The Anomaly Detection Settings dialog box appears.

The detector tree is displayed in the left area of the dialog box; the right area is empty.

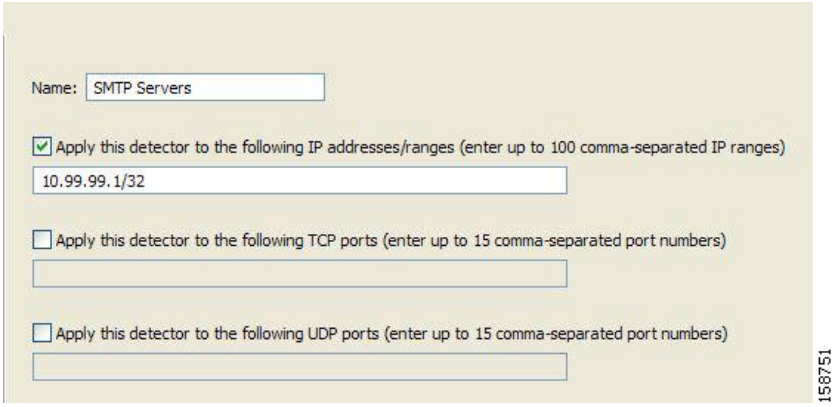
Figure 257: Detector Tree



Step 2 In the detector tree, select a detector.

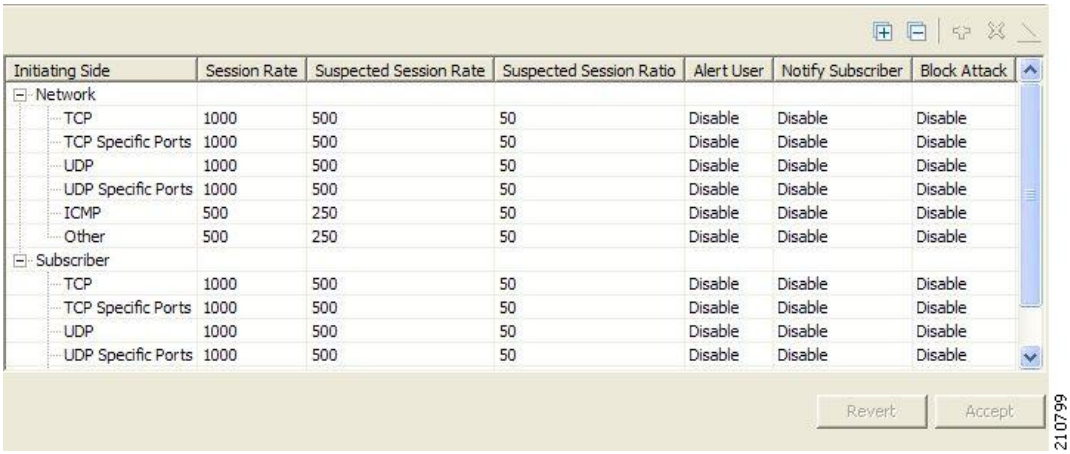
The detector parameters are displayed in the upper right area of the dialog box.

Figure 258: Detector Parameters



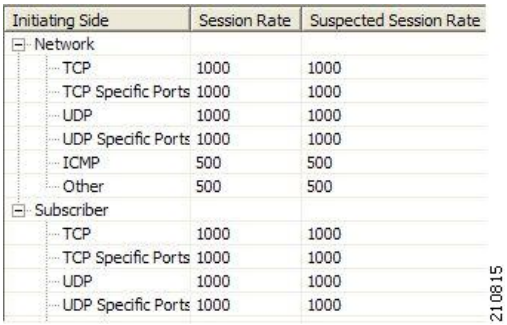
The anomaly types defined for a detector are listed in the lower right area of the dialog box, together with the value of each parameter. The following screen capture shows the default parameter values for the Scan/Sweep default detector.

Figure 259: Detector Defined Anomaly Types



If unidirectional classification is enabled, the Suspected Session Rate is set equal to the Session Rate, which effectively disables anomaly detection by the suspected session trigger.

Figure 260: Session Rate to Suspected Session Rate Comparison



Step 3 Click **OK**.
The Anomaly Detection Settings dialog box closes.

Adding Anomaly Detectors

A service configuration can contain up to 100 anomaly detectors.

You define IP address ranges and TCP and UDP ports for the new detector, and one anomaly type.

After you have defined the detector, you can add other anomaly types (see Editing Anomaly Detectors).

Procedure

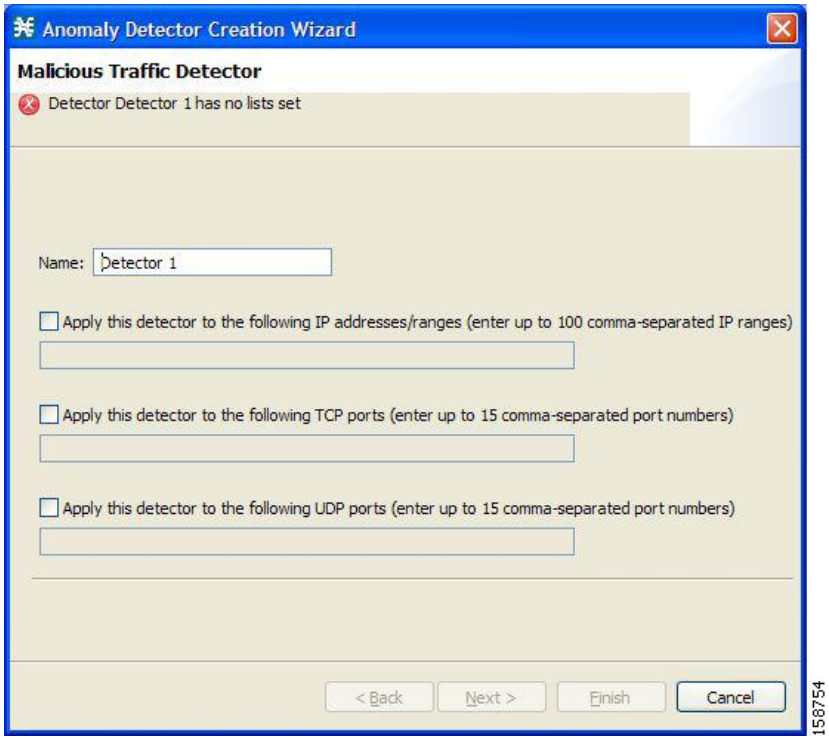
Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click **Configure**.
The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector category.

Step 3 Click the Add icon.

The Anomaly Detector Creation wizard appears, open to the Malicious Traffic Detector page.

Figure 261: Anomaly Detector Creation Wizard - Malicious Traffic Detector



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

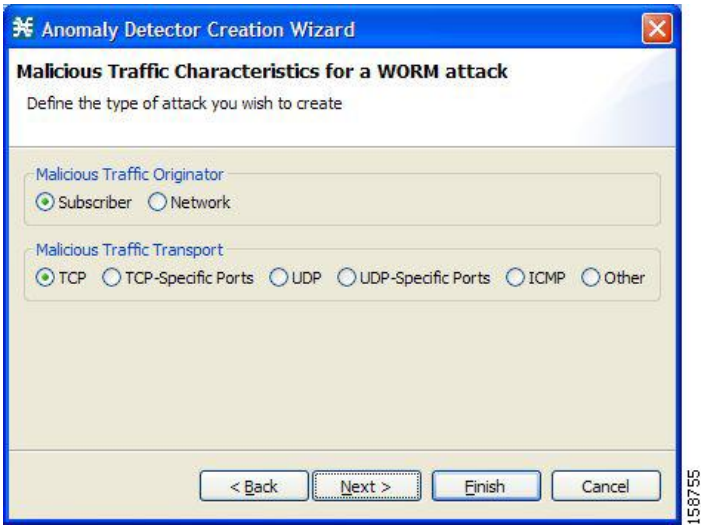
Step 5 Check one or more of the check boxes to limit the scope of the detector. The relevant fields are enabled.

Step 6 Enter lists of IP addresses or ports in the relevant fields.

Step 7 Click Next .

The Malicious Traffic Characteristics for a WORM attack page of the Anomaly Detector Creation wizard opens.

Figure 262: Malicious Traffic Characteristics for a Worm Attack



Step 8 Depending on the detector type that you are defining, select the originating side or the target side.

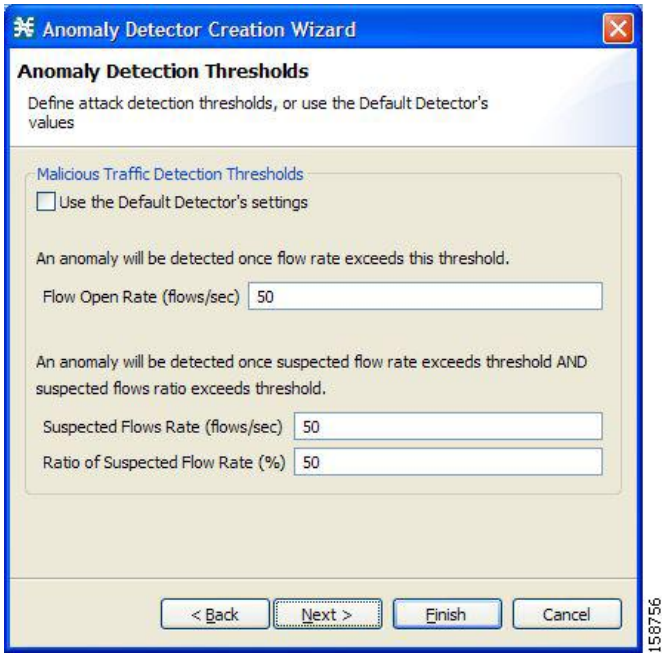
- If you are defining a Scan/Sweep detector or a DoS detector, select the originating side for the anomaly type you are defining.
- If you are defining a DDoS detector, select the target side for the anomaly type you are defining.

Step 9 Select a transport type for the anomaly type that you are defining.

Step 10 Click Next .

The Anomaly Detection Thresholds page of the Anomaly Detector Creation wizard opens.

Figure 263: Anomaly Detection Thresholds



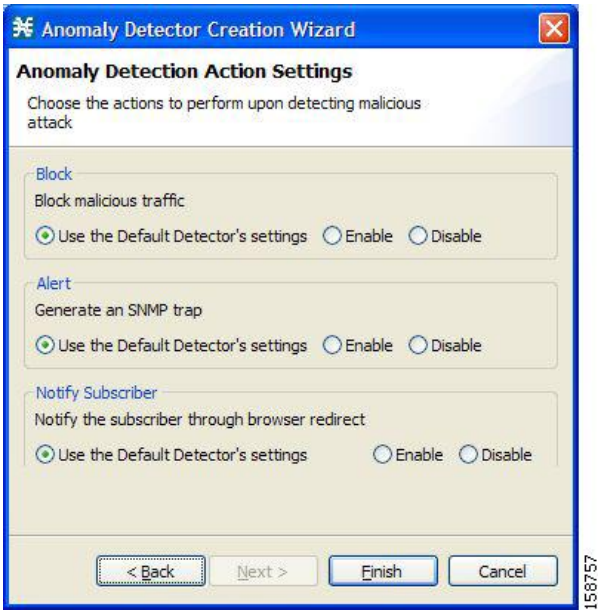
Step 11 Set the detector settings for this anomaly type.

- To use the setting for the default detector, check the Use the Default Detector's settings check box.
- Enter values in the Flow Open Rate, Suspected Flows Rate, and Ratio of Suspected Flow Rate fields.

Step 12 Click Next .

The Anomaly Detection Action Settings page of the Anomaly Detector Creation wizard opens.

Figure 264: Anomaly Detection Action Settings



Step 13 Select Block, Alert, and Notify Subscriber actions.

Step 14 Click Finish .
The Anomaly Detector Creation wizard closes.

The new detector is added to the detector tree.

You can now add additional anomaly types to the detector. See Editing Anomaly Detectors .

Editing Anomaly Detectors

You can perform the following actions on a user-defined anomaly detector:

- Edit detector parameters.
- Edit anomaly types.
- Add anomaly types.
- Delete anomaly types.
- Change the order of the detectors in the detector tree.

For each detector category, detectors are checked, *bottom-up,* in the order that they are listed in the detector tree; the default detector is checked last.

You can edit the anomaly types of the three default detectors.

Editing Detector Parameters

Procedure

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click Configure .
The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector.
The detector parameters are displayed in the upper right area of the dialog box.

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

Step 4 Check or uncheck the IP address range and ports check boxes.

Step 5 Enter or modify lists of IP addresses or ports in the relevant fields.

Step 6 Click OK.
The Anomaly Detection Settings dialog box closes.

Your changes are saved.

Editing Anomaly Types

Procedure

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click Configure .
The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector.
Information about the anomaly types is displayed in the lower right area of the dialog box.

Step 3 Double-click an anomaly type.
The Anomaly Detector Creation wizard appears, open to the Anomaly Detection Thresholds page (see Adding an Anomaly Type , on page 392 section).

Step 4 Set the detector settings for this anomaly type.
Do one of the following:

- To use the setting of the default detector, check the Use the Default Detector's settings check box.
- Change the values in the Flow Open Rate, Suspected Flows Rate, and Ratio of Suspected Flow Rate fields.

Step 5 Click Next.
The Anomaly Detection Action Settings page of the Anomaly Detector Creation wizard opens.

Step 6 Change Block, Alert, and Notify Subscriber actions.

Step 7 Click Finish .
The Anomaly Detector Creation wizard closes. The anomaly type is updated with your changes.

Step 8 Repeat Steps 3 to 7 (or Steps 2 to 7) for other anomaly types.

Step 9 Click OK.
The Anomaly Detection Settings dialog box closes.

Adding an Anomaly Type

Procedure

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click Configure .
The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector.
The anomaly types are listed in the lower right area of the dialog box.

Step 3 Click the Create New Detector Item Under Detector Items Feature  icon.
The Anomaly Detector Creation wizard appears, open to the Malicious Traffic Characteristics for a WORM attack page (see Adding Anomaly Detectors , on page 386 section).

Step 4 Select an origin for the anomaly type you are defining.

Step 5 Select a transport type for the anomaly type you are defining.

Step 6 Click Next .
The Anomaly Detection Thresholds page of the Anomaly Detector Creation wizard opens.

Step 7 Set the detector settings for this anomaly type.

- To use the settings of the default detector, check the Use the **Default Detector's settings** check box.
- Enter values in the Flow Open Rate, Suspected Flows Rate, and Ratio of Suspected Flow Rate fields.

Step 8 Click Next .
The Anomaly Detection Action Settings page of the Anomaly Detector Creation wizard opens.

Step 9 Select Block, Alert, and Notify Subscriber actions.

Step 10 Click Finish.
The Anomaly Detector Creation wizard closes.

The new anomaly type is added to the anomaly type list.

Step 11 Repeat Steps 3 to 10 (or Steps 2 to 10) for other anomaly types.

Step 12 Click OK.
The Anomaly Detection Settings dialog box closes.

Deleting an Anomaly Type

Procedure

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click Configure .
The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector.
The anomaly types are listed in the lower right area of the dialog box.

Step 3 In the anomaly type list, select an anomaly type.

Step 4 Click the Delete icon.
The selected anomaly type is deleted from the anomaly type list.

Step 5 Repeat Steps 3 and 4 (or Steps 2 to 4) for other anomaly types.

Step 6 Click **OK**.
The Anomaly Detection Settings dialog box closes.

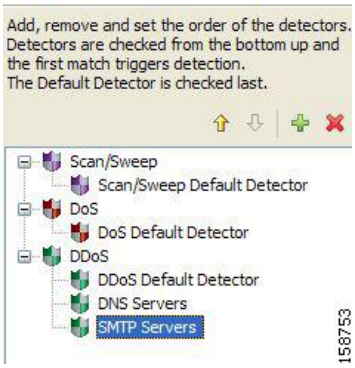
Changing the Order in which Detectors are Checked

Procedure

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click Configure .
The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select a detector.
The move up arrow, the move down arrow, or both are enabled, depending on the detectors location in the tree.

Figure 265: Detector Tree



Step 3 Using these navigation arrows, move the detector to its desired location.

Step 4 Repeat Steps 2 and 3 for other detectors.

Step 5 Click OK.
The Anomaly Detection Settings dialog box closes.

Your changes are saved.

Deleting Anomaly Detectors

You can delete any or all user-defined detectors.

You cannot delete the three default detectors.

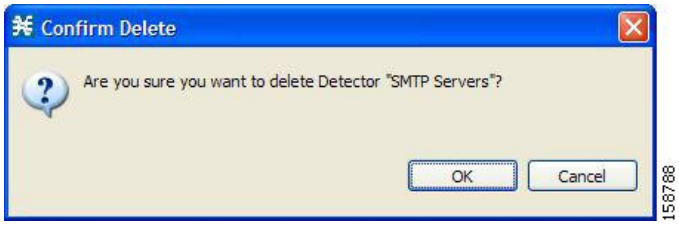
Procedure

Step 1 In the Service Security Dashboard, in the Anomaly Based Detection of Malicious Traffic pane, click Configure .
The Anomaly Detection Settings dialog box appears.

Step 2 In the detector tree, select one or more user-defined detectors.

Step 3 Click the Delete icon.
A Confirm Delete message appears.

Figure 266: Confirm Delete



Step 4 Click **OK**.
The selected detectors are deleted and are no longer displayed in the detector tree

Step 5 Click **OK** .
The Anomaly Detection Settings dialog box closes.

Managing Spam Detection Overview

The anomalous e-mail detection method monitors SMTP session rates for individual subscribers. A high rate of SMTP sessions from an individual subscriber is usually an indicator of malicious activity that involves sending e-mail (either mail-based viruses or spam-zombie activity).

This method works only if the system is configured in subscriber-aware or anonymous subscriber mode. This allows the Cisco SCE to accurately account the number of SMTP sessions generated per subscriber.

The detection method is based on the following:

- Typical broadband subscribers generate few SMTP sessions (at most a single session each time they send an e-mail message).
- Typical broadband subscribers normally use the SMTP server of the ISP (as configured in their mail client) as their only mail relay, and do not communicate with off-net SMTP servers.
- Spam zombies create many SMTP sessions, mainly to off-net servers (the mail servers of the destined recipient of the messages).

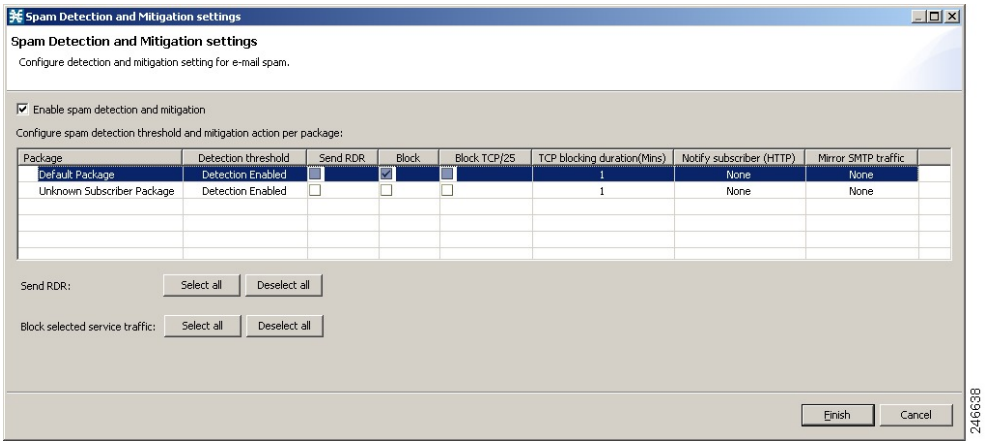
When configuring spam detection, you select an appropriate service to monitor. By default, this is the built-in SMTP service.

Configuring Spam Detection Settings

Procedure

Step 1 In the Service Security Dashboard, in the Spam Zombies and Email Viruses Detection pane, click Configure. The Spam Detection and Mitigation settings dialog box appears.

Figure 267: Spam Detection and Mitigation Settings



Step 2 (Optional) To disable spam detection, uncheck the Enable Spam detection and mitigation check box. All other fields are disabled. If you are disabling spam detection, continue at Step 6 .

Step 3 For each package, do the following:

a) Define the quota to be used for indicating anomalous e-mail activity.
We recommend that the values for these fields should be based on some baseline monitoring of subscriber activity.

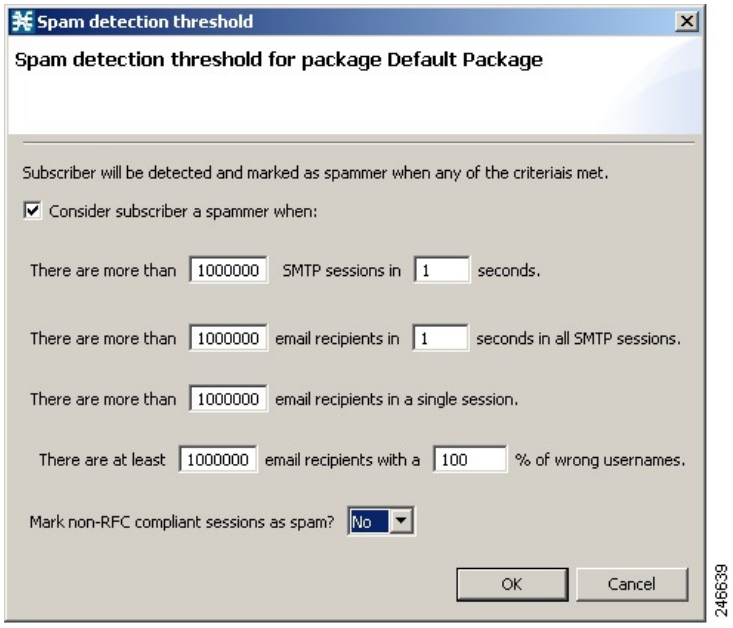
b) Click in the Detection threshold column.
A More (250619.jpg) button appears.

c) Click the More button.
The Spam Detection Threshold window appears.

d) Define when to consider the subscriber as a spammer.

e) Define whether to mark non-RFC compliant sessions as spam.
f) Click OK.

Figure 268: Spam Detection Threshold



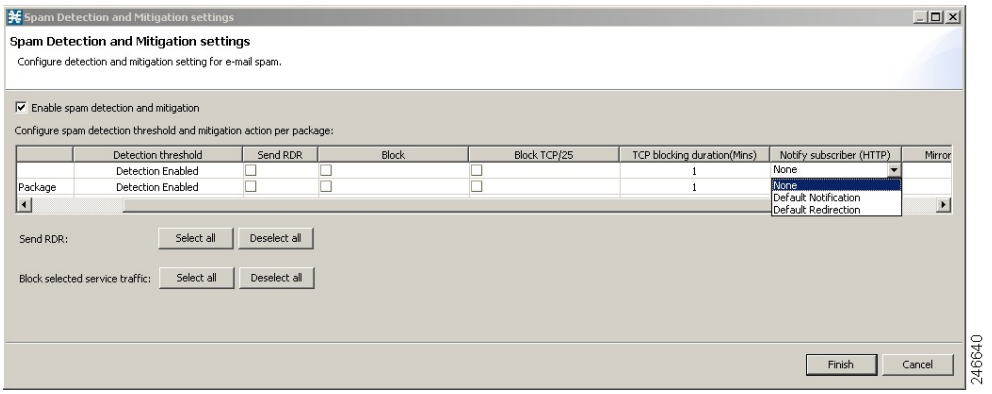
Step 4 Define one or more actions to be taken upon detecting mass-mailing activity.
Available actions are:

- Send RDR—Sends a Raw Data Record (RDR) to the Collection Manager (CM). A second RDR is sent when the status of the subscriber as a spammer is removed. The Collection Manager collects these RDRs in CSV files for logging purposes. Alternatively, you can implement your own RDR collectors to receive these RDRs and respond in real-time.
- Block—Blocks SMTP as a classified service.
- Block TCP/25—Blocks only the TCP port 25.
- TCP blocking duration (Mins)—Defines the duration for which the TCP port 25 should be blocked.
- Notify Subscriber (HTTP)—Redirects the subscriber browsing sessions to a captive portal presenting a message from the operator. This is done using “subscriber notification”. Options are None, Default Notification, Default Redirection.
- Mirror SMTP traffic—Diverts spam SMTP traffic to an inline spam detection service.

Note For the send RDR action, one RDR is sent when the subscriber is marked as a spammer and a second RDR is sent once the subscriber is no longer considered a spammer. However, when using the block and mirror actions, the action begins when the subscriber is marked as a spammer and is maintained until the subscriber is no longer considered a spammer.

Note Block SMTP Traffic and Mirror SMTP traffic cannot both be selected. If you select one, the other is disabled.

Step 5 If you selected Notify Subscriber (HTTP), choose or enter a notify subscriber.



Step 6 If you selected Mirror SMTP traffic, choose a server group.

Step 7 Click Finish.
The Spam Detection and Mitigation settings dialog box closes.

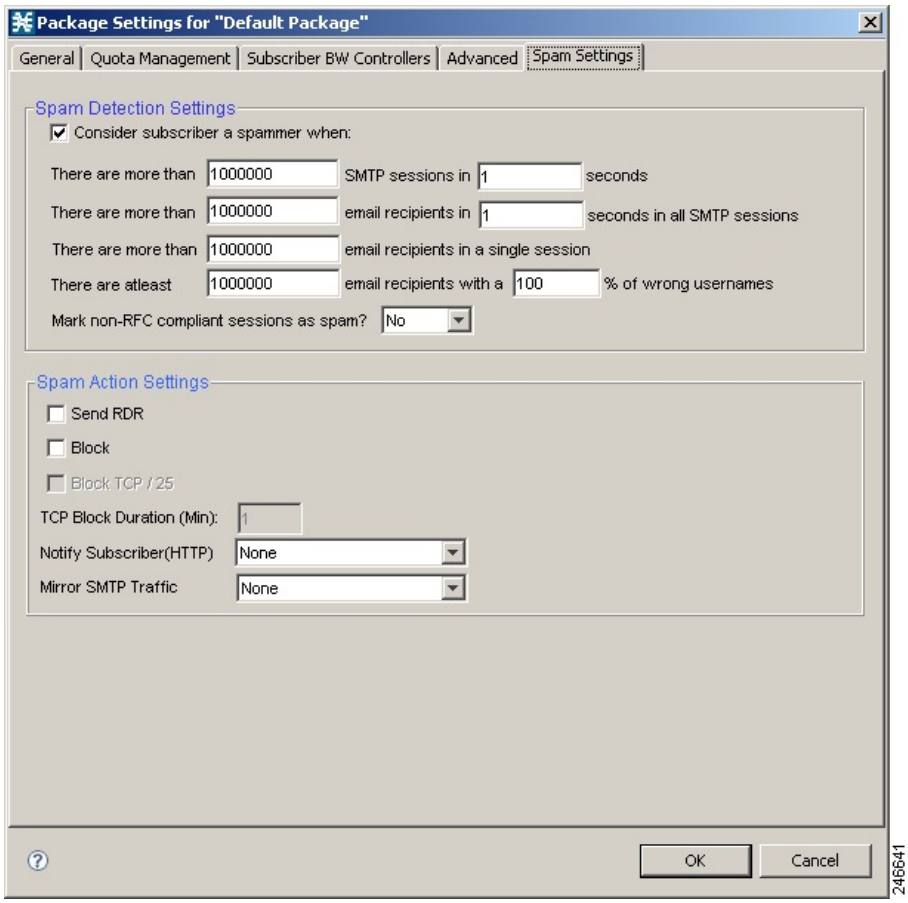
Configuring Outgoing Spam Mitigation Settings per Package from Subscriber Policies

Procedure

Step 1 In the Service Configuration Editor Policies tab, select a Package from the Subscriber Policies.

Step 2 Right-click on the Package and select Edit Package.
The Package Settings window appears.

Step 3 Click Spam Settings tab to view the Spam Detection Settings and Spam Action Settings.



Step 4 Select the Consider Subscriber a spammer when: check box to enable the spam detection.

Step 5 Define when to consider the subscriber a spammer and the actions to be taken.

Step 6 Click OK.

For more details on spam mitigation, see the Cisco Service Control Service Security: Outgoing Spam Mitigation Solution Guide.

Malicious Traffic Reports Overview

Information about detected traffic anomalies is stored in the Collection Manager database. You can use this information for network trending, detection of new threats, and tracking of malicious hosts or subscribers.

- Malicious Traffic Reports
- How to View a Service Security Report

Malicious Traffic Reports

A number of reports dealing with malicious traffic can be displayed in the SCA Reporter tool:

- Global reports:
  - Global Scan or Attack Rate
  - Global DoS Rate
  - Infected Subscribers
  - Infected Subscribers versus Active Subscribers
  - DoS Attacked Subscribers
  - Top Scanned or Attacked ports
- Individual subscriber or hosts reports:
  - Top Scanning or Attacking hosts
  - Top DoS Attacked hosts
  - Top DoS Attacked Subscribers
  - Top Scanning or Attacking Subscribers

Viewing a Service Security Report

Procedure

Step 1 In the Service Security Dashboard, in the relevant pane, click **View Report**.
A Choose a report dialog box appears, displaying a tree of relevant reports.

Step 2 Select a report from the report tree.

Step 3 Click **OK**.
The Choose a report dialog box closes.

The Reporter tool opens in the Console, and displays the requested report.

For information about manipulating and saving the report, see the “Working with Reports” chapter of Cisco Service Control Application Reporter User Guide.

Traffic Flow Filtering

Filter rules are part of service configurations. They allow you to instruct the Cisco SCE platform, based on a flow’s Layer 3 and Layer 4 properties, to:

- Bypass—Ignore the flow and transmit it unchanged.
- Quick forward—Duplicate the flow and send one copy directly to the transmit queue to ensure minimal delay. The second copy goes through the normal packet path.

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

If a filter rule applies to this traffic flow, the Cisco SCE platform passes the traffic flow to its transmit queues. No RDR generation or service configuration enforcement is performed; these flows do not appear in any records generated for analysis purposes and are not controlled by any rule belonging to the active service configuration.

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

A number of predefined filter rules are included in every new service configuration.



Note By default, some, but not all, of the predefined filter rules are active.

Flows of certain protocols can also be filtered according to the Layer 7 characteristics of the flow (see Advanced Service Configuration Options, on page 435 section). Like other filtered flows, Layer 7 filtered flows are not controlled, but can be classified and reported. The flows of the protocols that can be filtered are typically short and their overall volume is negligible. So filtering these protocols has little effect on network bandwidth and on the accuracy of the Cisco SCA BB reports.

Information About Traffic Filtering

For certain types of traffic, service providers may need to reduce the latency and jitter introduced by the Cisco SCE platform or even to bypass the Cisco SCE platform to avoid traffic control as well. Typically, such decisions are made for a portion of the traffic, to reduce latency for delay sensitive applications, such as voice, and to bypass mission-critical traffic, such as routing protocols. The Cisco SCA BB Filtered Traffic mechanism is used to address this need.



Note To reduce latency, Cisco SCE platform automatically handles most voice traffic. For details, seeAutomatic Quick Forwarding of Media Flows, on page 402 section.

The Cisco SCA BB Filtered Traffic Mechanism

The Cisco SCA BB Filtered Traffic mechanism reduces latency or completely bypasses portions of the traffic by defining filter rules that match relevant flows and assign the correct action to them. A filter rule matches a packet according to its Layer 3 and Layer 4 properties, such as IP address, port number, and DSCP ToS, as well as the Cisco SCE platform interface (subscriber or network) from which the packet arrived. For packets that match a filter rule, the following actions can be applied:

- Bypass the current packet (to reduce latency and avoid traffic control).

When this action is applied, the current packet is directly transmitted from the Cisco SCE platform without going through any service configuration processing or reporting. You must map the bypassed packet to a Class of Service (CoS) to assign it to one of the transmit queues of the Cisco SCE platform.

Possible values for CoS are BE, AF1, AF2, AF3, AF4, and EF; where EF implies high processing priority and the other classes imply normal processing priority.

- Quick forward the flow (to reduce latency).

When this action is applied, the current packet and all subsequent packets belonging to the same flow are duplicated and sent through two different paths: the original packet goes directly to the transmit queue, and thus has only a minimal delay, while a copy of the packet goes through the normal service configuration processing path for classification and reporting, and is then discarded.

- Assign the flow to the high priority processing input queue (to reduce latency).

Note Not all platforms support this option.

When this action is applied, the current packet and all subsequent packets belonging to the same flow enter the high priority processing input queue. They go through the normal service configuration processing path ahead of other packets that arrive simultaneously. You should map the flow to the EF CoS to assign it to the high processing priority transmit queue of the Cisco SCE platform.

Note In an MPLS environment, the Cisco SCE platform does not map the DSCP bits to the EXP bits of the MPLS header.

A filter rule can perform DSCP ToS marking (by changing the DSCP ToS field of the packet) of the matched traffic with any of the above actions.

Note DSCP ToS marking and the assignment to CoS only take place when the operational mode of the system is Full Functionality (see System Operational Mode , on page 434 section).

The Cisco SCE processes the traffic based on the Class of Service (CoS). Possible values for CoS are BE, AF1, AF2, AF3, AF4, and EF; where EF implies high processing priority and the other classes imply normal processing priority.

In , if there are 4 output queues—EF, AF n ,AF1, and BE, this is how the queues are prioritized:

- EF—Gets the highest priority and strictly gets priority over all other queues.
- AF1 and AF n (AF2, AF3, AF4)—Gets the weighted priority on top of AF1. For each n packets of AF n , one packet is sent for AF1. The value of n can be configured from the FPGA. The default value is 3.
- BE—Gets lowest priority. BE packets are transmitted only if packets for transmission are not available in other queues.

The Cisco SCE transmits only the received packet and do not generate the traffic internally; other than rarely transmit inject for reset or redirect. So, there can never be a long time in which lower priority queues are starved.

When there are only buckets—EF and the rest. In CoS other than EF (AF1,AF2,AF3,AF4,BE), the order of priority would be AF1 > AF2 > and so on. However, the bandwidth is allocated in the order EF > AF n > AF1 > BE. Queues AF2, AF3, and AF4 would have the same weight.

Filter Rule Actions

The Bypass and Quick forward actions apply to different scopes of traffic:

- The Bypass action only bypasses the current packet; every subsequent packet of the same flow goes through the Filtered Traffic mechanism. This means, for example, that when traffic is to be bypassed based on its destination port number, two rules should be created to match packets from both sides of a bidirectional flow.
  For example, to bypass all traffic to destination port 23, two filter rules are needed, one for packets arriving from the subscriber side addressed to network side port 23, and another for packets arriving from the network side addressed to subscriber side port 23.
- The Quick forward action is applied to the entire flow; once identified, all subsequent packets do not go through the filter rule mechanism, instead going through normal service configuration processing. A packet may match more than one filter rule. If both Bypass and Quick forward are matched, the packet/flow is bypassed with minimum delay. Furthermore, if only Bypass is matched, the packet/flow is also be bypassed with minimum delay.

Filter Rules and Service Rules

Filter rule actions to reduce latency allow the flow to be controlled by the Cisco SCE platform. This means that the flow can be blocked or given limited bandwidth if it matches a service rule. For example, if a filter rule is applied to reduce latency, but a service configuration rule is applied to block the same traffic, the traffic is blocked.

The Bypass action is designed to avoid service configuration processing; bypassed traffic is not affected by service rules.

Automatic Quick Forwarding of Media Flows

The Cisco SCE platform reduces the latency of delay-sensitive voice and video media flows by applying the quick-forwarding action to SIP, MGCP, H323, Skinny, and RTSP media flows during classification. When a media flow is classified as being of one of these types, it is subjected to quick forwarding immediately.

The Cisco SCE platform does this automatically, regardless of filter rule configuration. These media flows might still be blocked or given limited bandwidth if they match a service rule.

Filtering L2TP Traffic

If you know the version of the L2TP tunnel that is being used, configure the relevant filters. If you do not know the version, enable filter for both type of tunnels (L2TPv2 and L2TPv3).



Note The L2TPv3 data encapsulation is done directly over IP with protocol ID 115. Cisco SCA BB provides a filter for this type of traffic and you can enable it from Cisco SCA BB. However, L2TPv2 protocol data encapsulation is done over UDP protocol at Layer 4 with default destination port 1701. Cisco SCA BB does not provide any filter for this type of traffic. To filter L2TPv2 traffic, create a new filter with the transport type as UDP and destination UDP port value as 1701.

Viewing Filter Rules for a Package

You can view a list of the filter rules included in a service configuration.

The listing for each filter rule includes the name, the status, and a brief description (generated by the system) of the rule.

To see more information about a filter rule, open the Edit Filter Rule dialog box (see Editing Filter Rules).

Procedure

In the Policies tab, select the Filtered Traffic node.
A list of all filter rules is displayed in the right (Rule) pane.

Figure 269: Filter Rules

Setting Flexible Configuration of Port based Filters

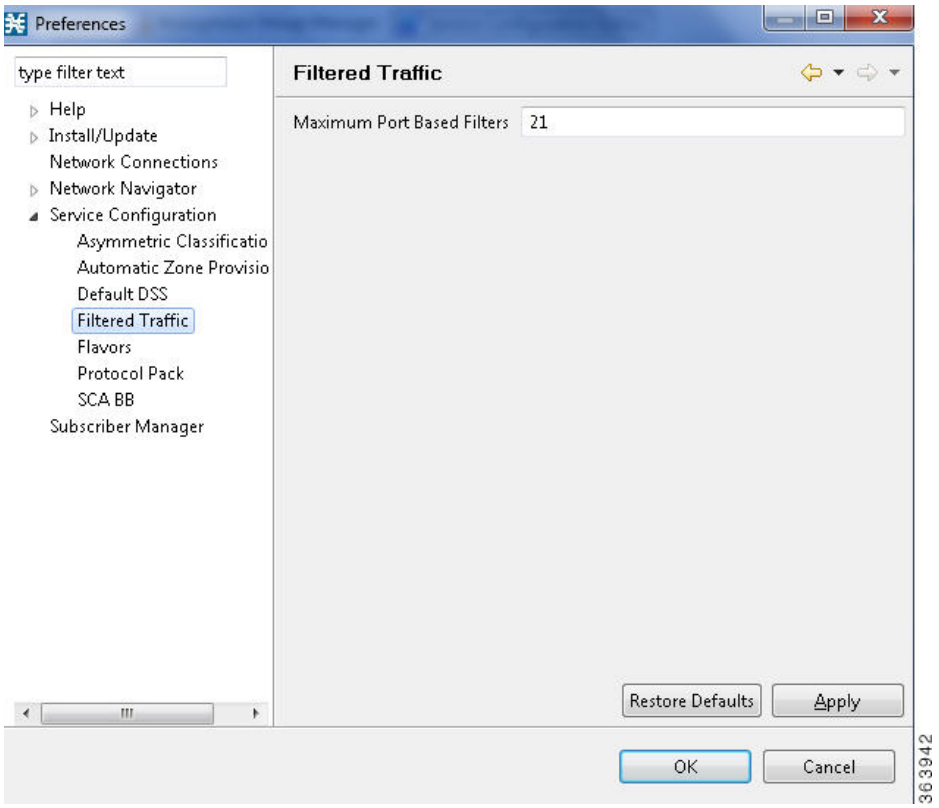
Procedure

Step 1 Choose **Windows** > **Preferences**.

Step 2 In the Preferences window, expand the Service Configuration.

Step 3 Click **Filtered Traffic**.

Step 4 For SCE 8000 - Enter the value of the port based filters. The valid integer values of the port based filters range between 21 and 50. The default value is 21.



Step 5 Click **Apply**.

Step 6 Click **OK**.
SCE 8000 Calculation: The number of IP based flow filters is reduced, based on the configured flow filters count. For example, if the number of port based flow filter count is increased as 27, the result is as follows:

- Port Based Flow Filter : 27 rules (34 - 60)
- IP based Flow Filter : 33 rules (1 - 33)

Adding Filter Rules

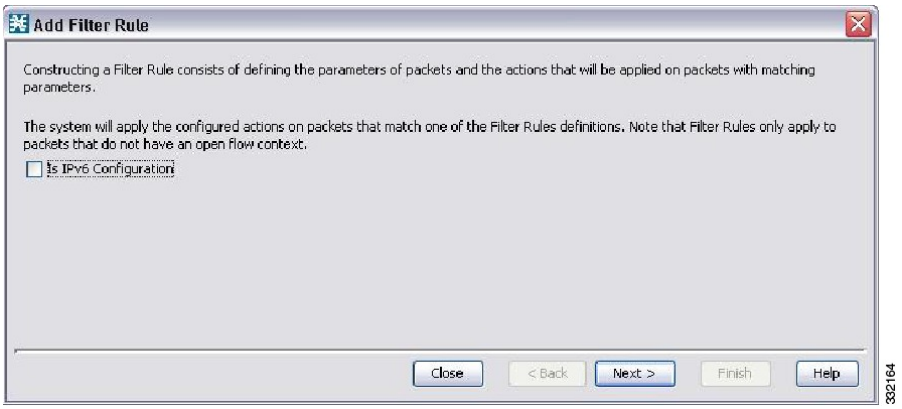
The Add Filter Rule wizard guides you through the process of adding a filter rule.

Procedure

Step 1 In the Policies tab of Service Configuration Editor window, select the Filtered Traffic node.

Step 2 Click  (Add Rule) in the right (Rule) pane.
The Add Filter Rule wizard appears.

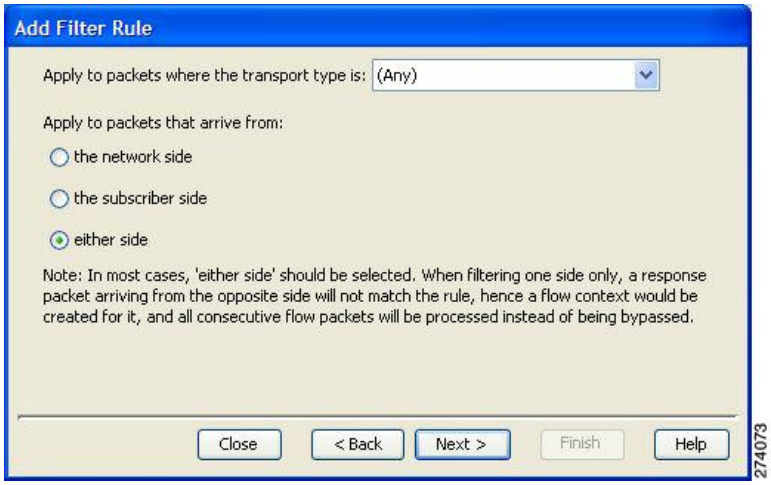
Figure 270: Add Filter Rule



Step 3 Click Next.

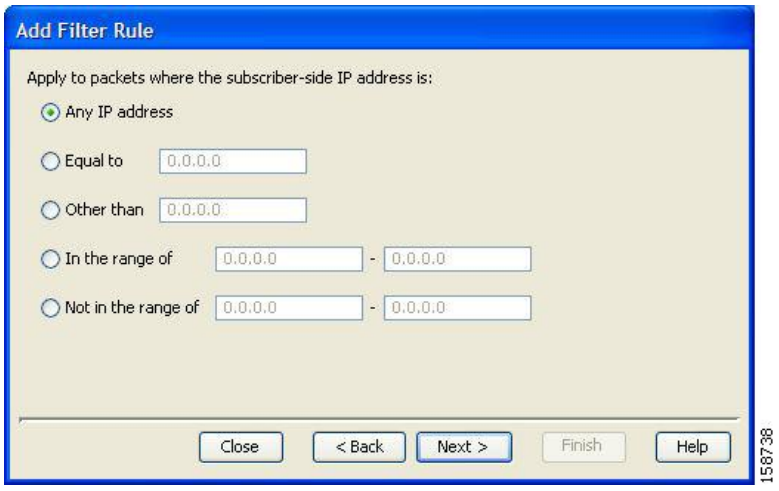
The Transport Type and Direction screen of the Add Filter Rule wizard appears.

Figure 271: Transport Type and Direction



Step 4 Select the transport type and initiating side and click Next .
The Subscriber-Side IP Address screen of the Add Filter Rule wizard appears.

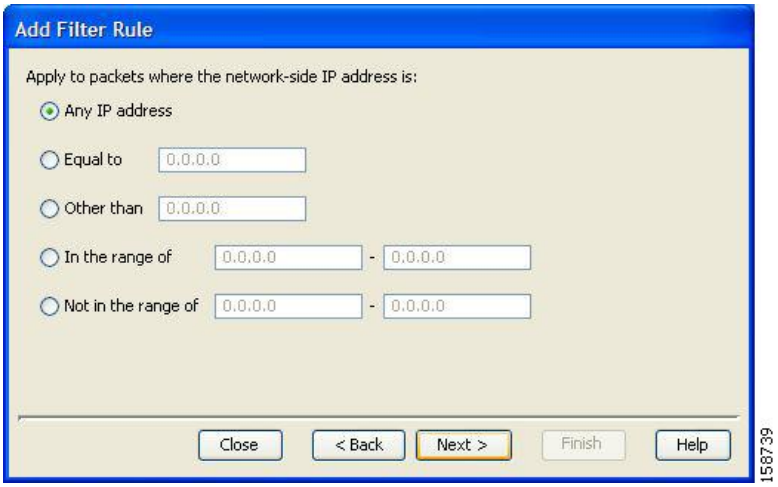
Figure 272: Subscriber-Side IP Address



Step 5 Define the subscriber-side IP address and click Next.

The Network-Side IP Address screen of the Add Filter Rule wizard appears.

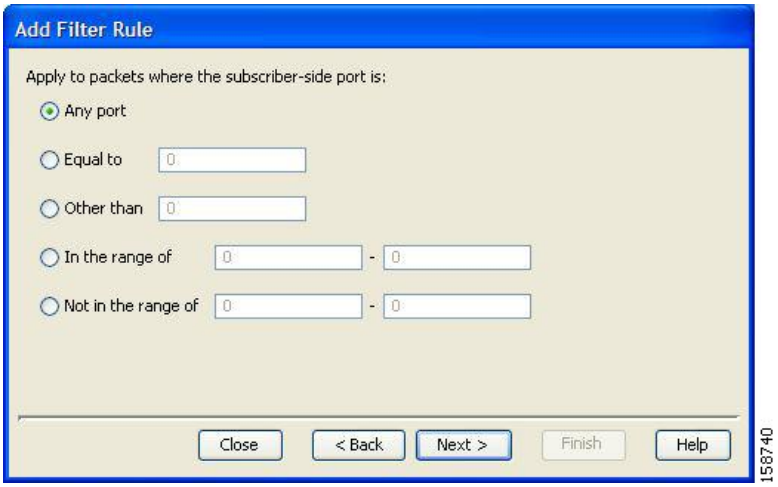
Figure 273: Network-Side IP Address



Step 6 Define the network-side IP address and click Next.
If the transport type selected in Step 4 was not TCP or UDP, the ToS screen of the Add Filter Rule wizard appears. Go to Step 9.

If the transport type selected in Step 4 was TCP or UDP, the Subscriber-Side Port screen of the Add Filter Rule wizard appears.

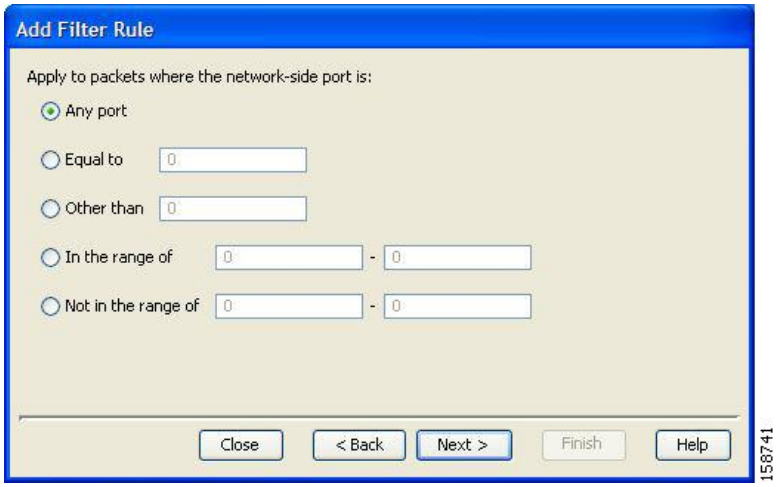
Figure 274: Subscriber-Side Port



Step 7 Define the subscriber-side port and click Next.

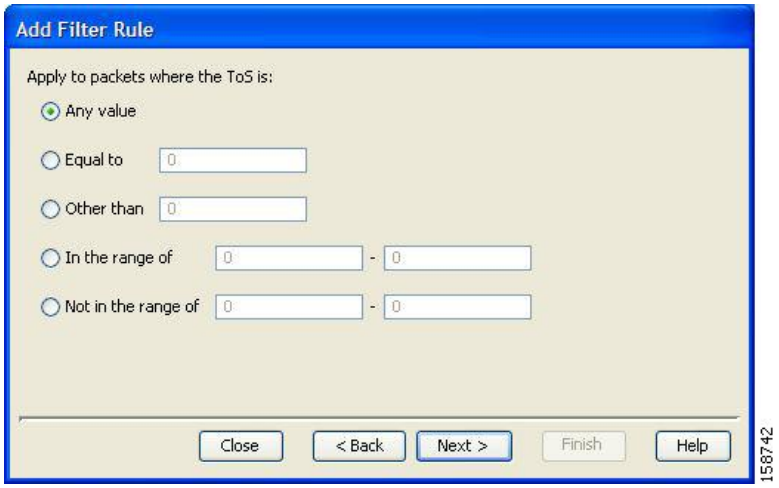
The Network-Side Port screen of the Add Filter Rule wizard appears.

Figure 275: Network-Side Port



Step 8 Define the network-side port and click Next.
The Type of Service (ToS) screen of the Add Filter Rule wizard appears.

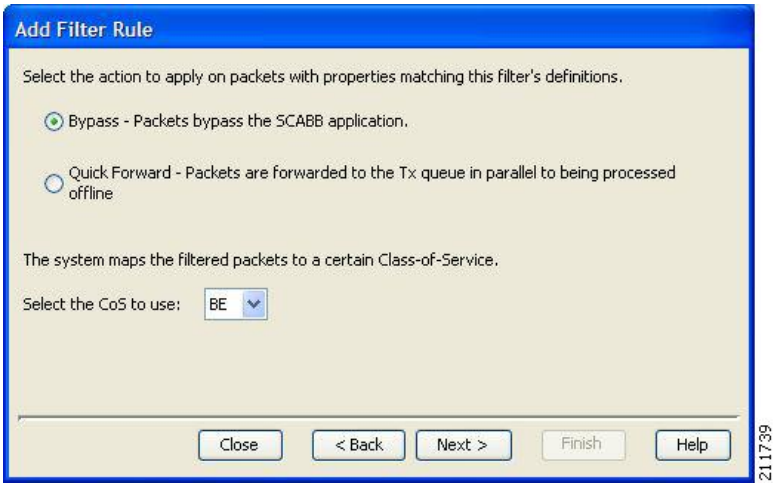
Figure 276: ToS



Step 9 Define the ToS and click Next.
The acceptable values for ToS are 0 to 63.

The Action and Class-of-Service screen of the Add Filter Rule wizard appears.

Figure 277: Action and Class-of-Service

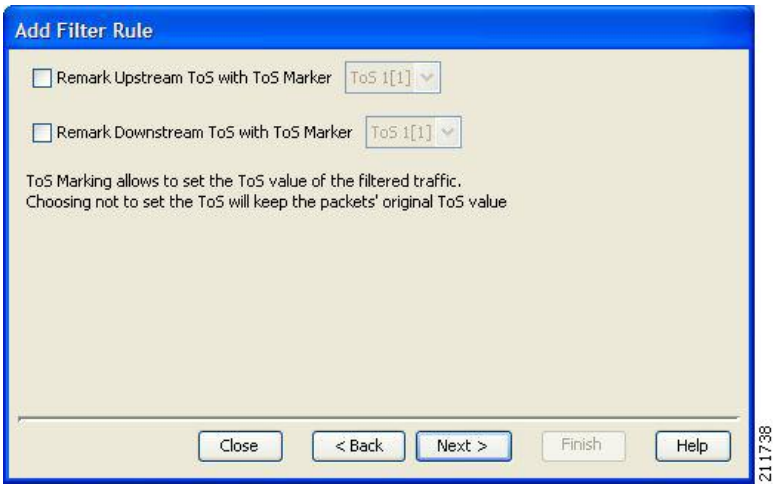


Step 10 Select the radio button for the required action.

- Bypass —Packets that match this filter rule are not passed to Cisco SCA BB.
- Quick Forward —The Cisco SCE platform ensures low latency for packets that match this filter rule (use for delay sensitive flows). Packets are duplicated and passed to Cisco SCA BB for processing.

Step 11 Select a Class-of-Service value, and click Next.
The ToS Marking screen of the Add Filter Rule wizard appears.

Figure 278: ToS Marking

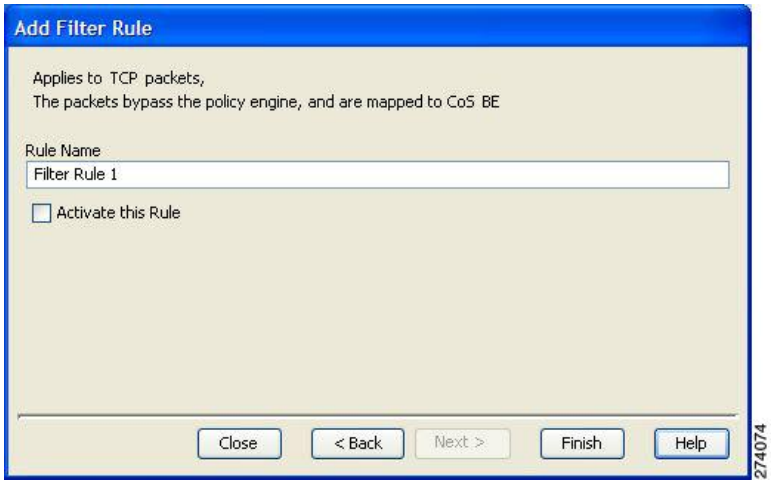


Step 12 (Optional) To change the DSCP ToS marker of packets in the filtered traffic, check the Remark Upstream ToS with ToS Marker and Remark Downstream ToS with ToS Marker check boxes, as required, select the required ToS marker from the drop-down list, and click Next .

- Disabling directional DSCP ToS marking in the ToS Marking Settings dialog box (see How to Manage DSCP ToS Marker Values , on page 358 section) overrides DSCP ToS marking in that direction by a filter (that is, the DSCP ToS value are not changed). In this case, the Problems View displays a Warning.
- If you filter for a flow in one direction in Step 4 but select ToS marking in the other direction in this Step, the filter rule is created, but no DSCP ToS remarking occurs. In this case, the Problems View displays a Warning.
- If you select Quick Forward in the previous Step, Cisco SCA BB receives the original package and processes it. That is, the application see the original DSCP ToS value regardless of the ToS marking action selected in the filter rule.

The Finish page of the Add Filter Rule wizard opens.

Figure 279: Finish



Step 13 In the Rule Name field, enter a unique name for the new filter rule.

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

Step 14 (Optional) To activate the filter rule, check the Activate this rule check box. Traffic is filtered according to the rule only when it is activated.

Step 15 Click Finish.
The Add Filter Rule wizard closes.

The filter rule is added and is displayed in the Filter Rule table.

Adding Filter Rules for IPv6 Configuration

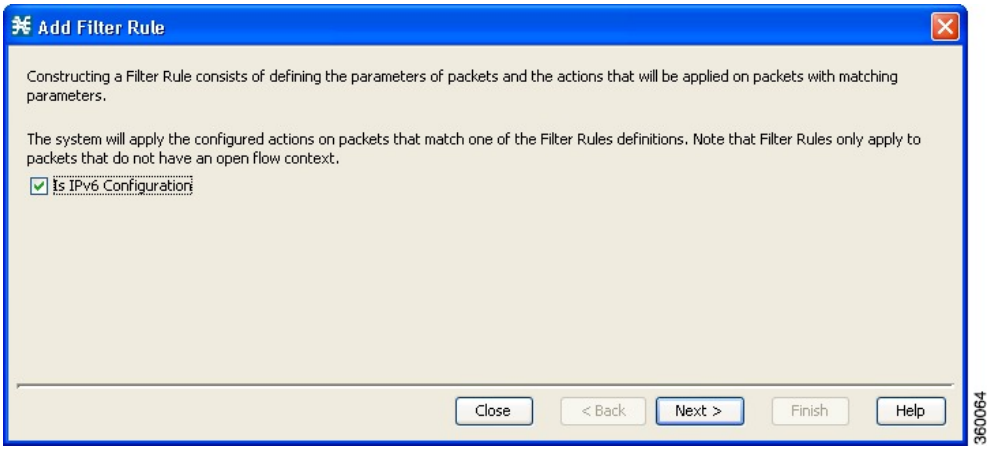
The Add Filter Rule wizard guides you through the process of adding a filter rule for IPv6 configuration.

Procedure

Step 1 In the Policies tab of Service Configuration Editor window, select the Filtered Traffic node.

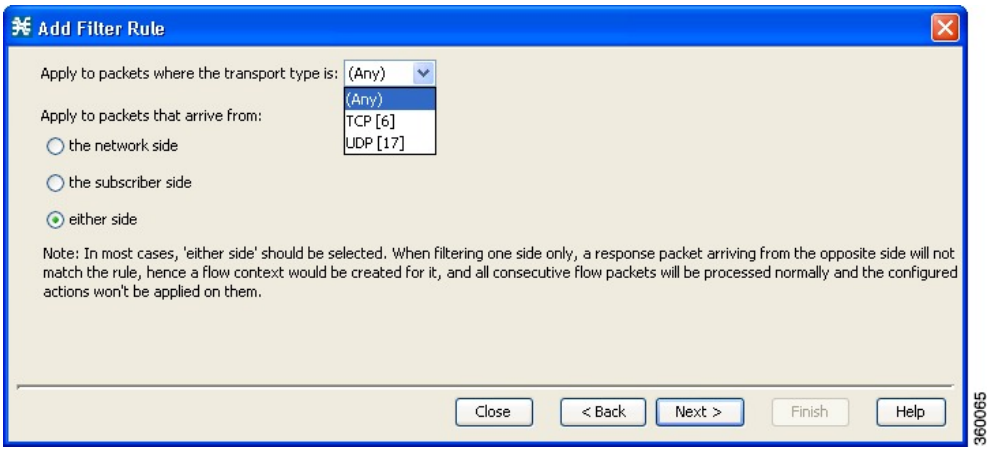
Step 2 Click Add Rule  in the right (Rule) pane.
The Add Filter Rule wizard appears.

Figure 280: Add Filter Rule Wizard



Step 3 Select the Is IPv6 Configuration check box and click Next.
The Transport Type and Direction screen of the Add Filter Rule wizard appears.

Figure 281: Transport Type and Direction

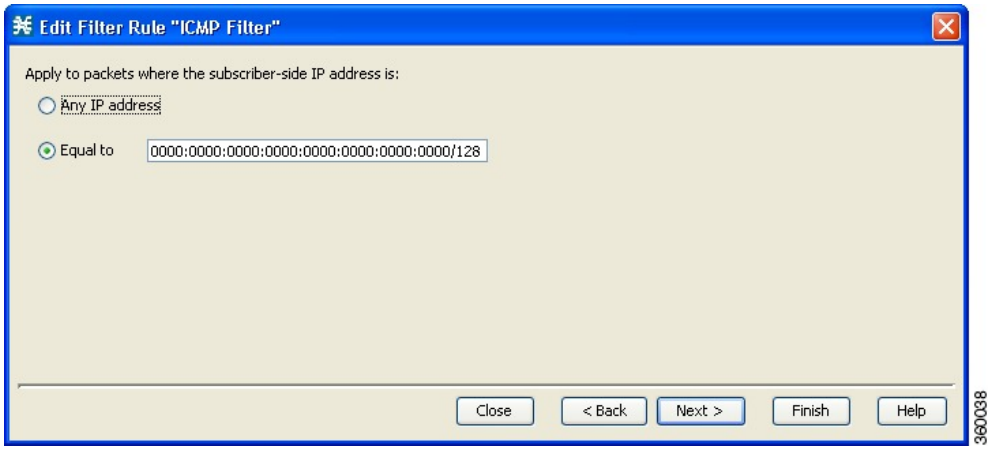


Step 4 Select the transport type and the initiating side and click **Next**.

Note The transport type drop-down will contain only the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) values.

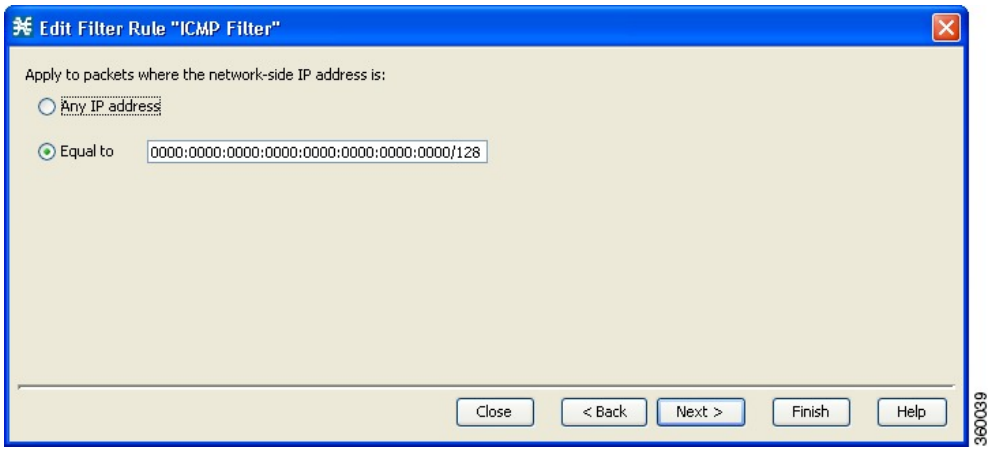
The Subscriber-Side IP Address screen of the Add Filter Rule wizard appears.

Figure 282: Subscriber-Side IP Address



Step 5 Define the subscriber-side IP address and click Next .
The Network-Side IP Address screen of the Add Filter Rule wizard appears.

Figure 283: Network-Side IP Address

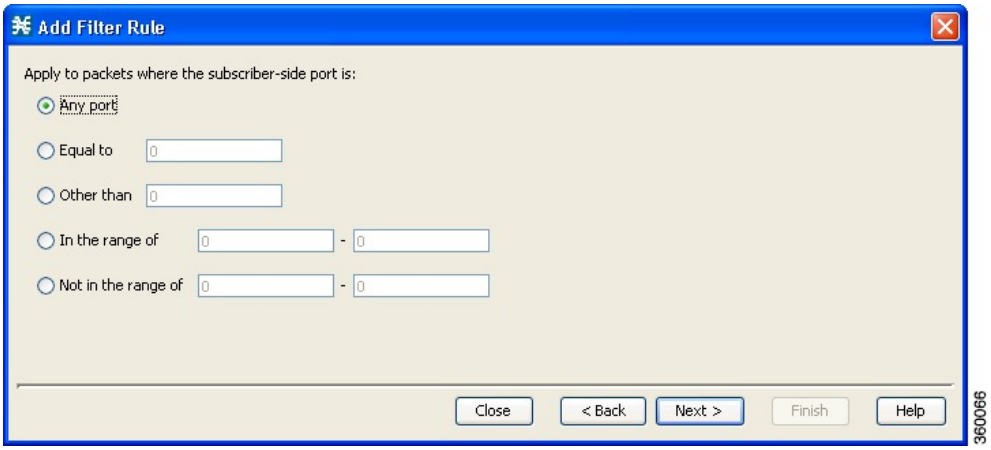


Step 6 Define the network-side IP address and click Next .
You can use 128-bit masks for the subscriber side IP addresses and the network side IP addresses.

If the transport type selected in Step 4 was not TCP or UDP, the ToS screen of the Add Filter Rule wizard appears. Go to Step 9.

If the transport type selected in Step 4 was TCP or UDP, the Subscriber-Side Port screen of the Add Filter Rule wizard appears.

Figure 284: Subscriber-Side Port



Step 7 Define the subscriber-side port and click Next .
The Network-Side Port screen of the Add Filter Rule wizard appears.

Figure 285: Network-Side Port



Step 8 Define the network-side port and click Next.
The ToS screen of the Add Filter Rule wizard appears.

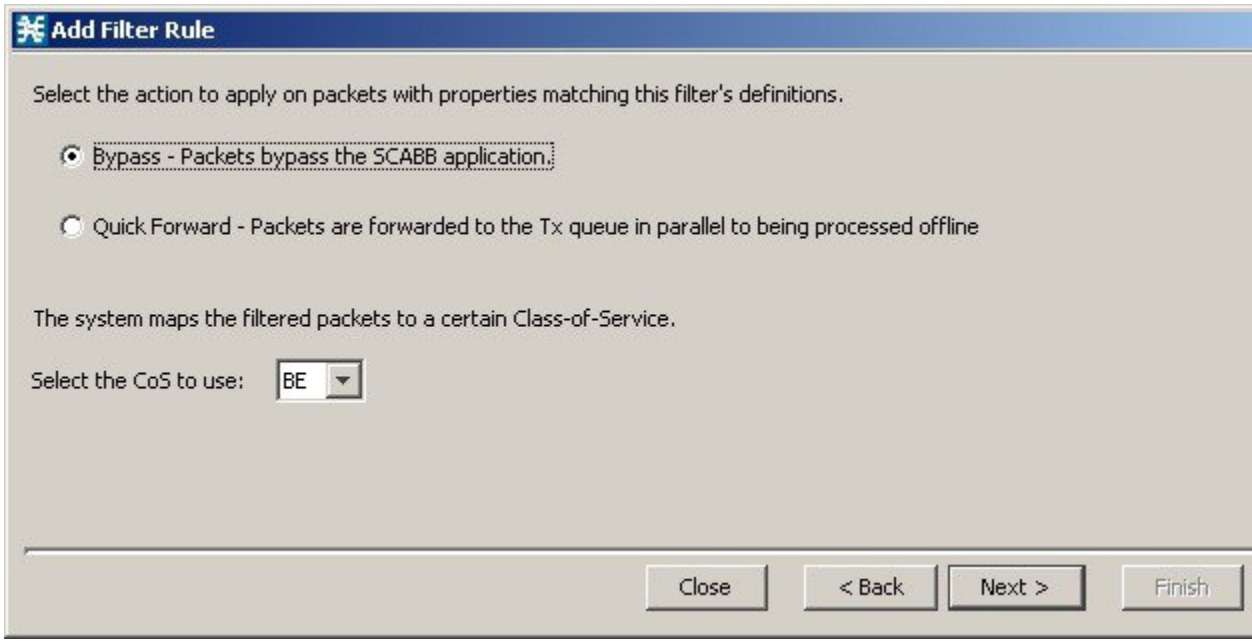
Figure 286: ToS



Step 9 Define the ToS and click Next .
The acceptable values for ToS are 0 to 63

The Action and Class-of-Service screen of the Add Filter Rule wizard appears.

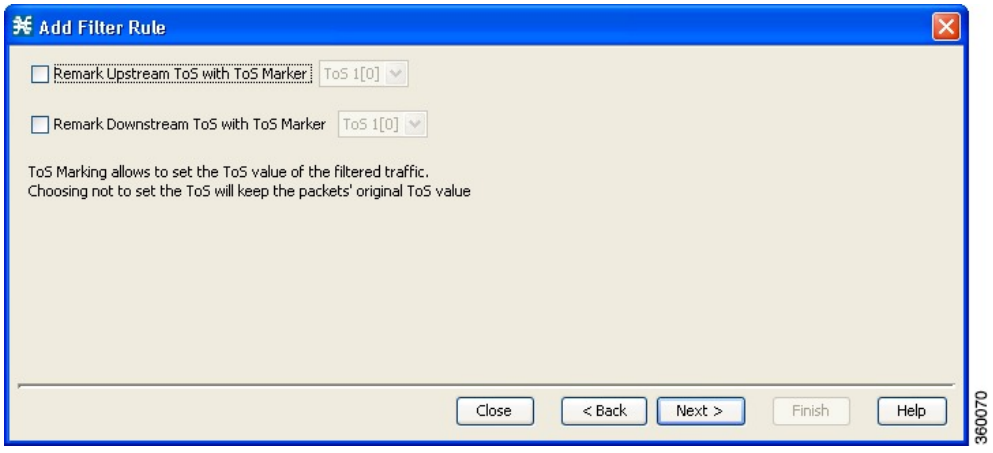
Figure 287: Action and Class-of-Service



Step 10 Select the following radio button for the corresponding action:

Step 11 Select a Class-of-Service value, and click Next .
The ToS Marking screen of the Add Filter Rule wizard appears.

Figure 288: ToS Marking

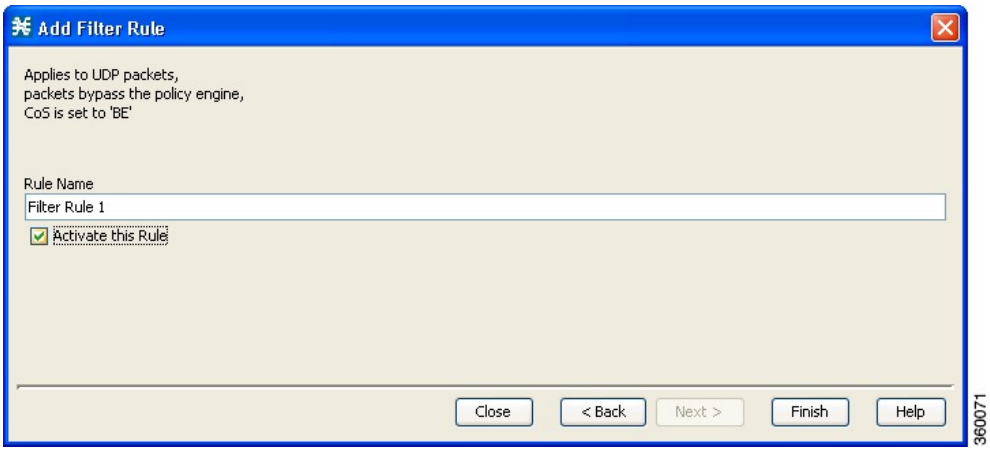


Step 12 (Optional) To change the DSCP ToS marker of packets in the filtered traffic, check the Remark Upstream ToS with ToS Marker and Remark Downstream ToS with ToS Marker check boxes, select the required ToS marker from the drop-down list, and click **Next**.

- Disabling the directional DSCP ToS marking in the ToS Marking Settings dialog box (see How to Manage DSCP ToS Marker Values , on page 358 section) overrides the DSCP ToS marking in that direction by a filter (that is, the DSCP ToS value is not changed). In this scenario, the Problems View displays a warning message.
- If you apply a filter for a flow in one direction in Step 4, but select ToS marking in the other direction in this step, the filter rule is created, but no DSCP ToS remarking occurs. In this scenario, the Problems View displays a warning message.

The Finish screen of the Add Filter Rule wizard appears.

Figure 289: Finish

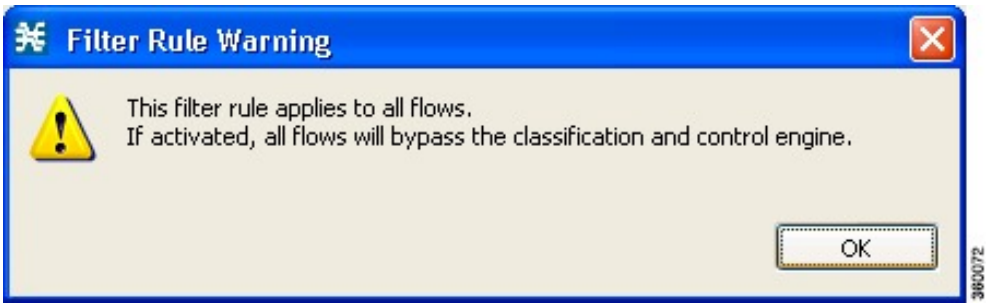


Step 13 In the Rule Name field, enter a unique name for the new filter rule.
Note You can use the default name for the filter rule. We recommend that you enter a meaningful name.

Step 14 (Optional) To activate the filter rule, check the Activate this rule check box. Traffic is filtered according to the rule only when it is activated.

Step 15 Click Finish.
The Add Filter Rule wizard closes. The Filter Rule Warning message is displayed.

Figure 290: Filter Rule Warning Message



The filter rule that has been added is displayed in the Filter Rule table.

Editing Filter Rules

You can view and edit the parameters of a filter rule.

Procedure

Step 1 In the Policies tab of Service Configuration Editor window, select the Filtered Traffic node.
A list of all filter rules is displayed in the right (Rule) pane.

Step 2 Select a rule in the Filter Rule table.

Step 3 Click the Edit Rule  icon.
The Introduction page of the Edit Filter Rule wizard appears.

The Edit Filter Rule wizard is the same as the Add Filter Rule wizard.

Step 4 Follow the instructions in the section Adding Filter Rules , on page 404, Steps 4 to 14.

Step 5 Click Finish.
The filter rule is changed and the corresponding changes are displayed in the Filter Rule table.

Deleting Filter Rules

You can delete filter rules. This is useful, for example, when you want the system to resume handling the IP addresses and their attributes according to the individual rules that were previously defined for each subscriber IP address.

Procedure

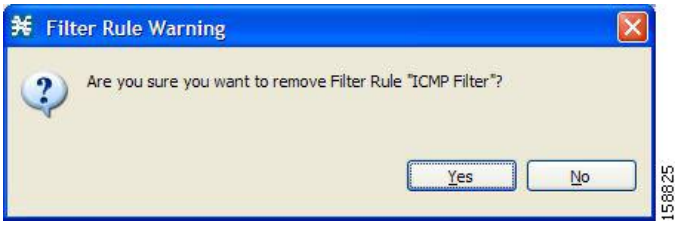
Step 1 In the Policies tab, select the Filtered Traffic node.
A list of all filter rules is displayed in the right (Rule) pane.

Step 2 Select a rule in the Filter Rule table.

Step 3 Click the Delete Rule  (158940.jpg) icon.

A Filter Rule Warning message is displayed.

Figure 291: Filter Rule Warning



Step 4 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 you can reactivate the filter rule at a later date.

Procedure

Step 1 In the Policies tab, select the Filtered Traffic node.
A list of all filter rules is displayed in the right (Rule) pane.

Step 2 Select a rule in the Filter Rule table.

Step 3 To activate the rule, check the Active check box.

Step 4 To deactivate the rule, uncheck the Active check box.

Step 5 Repeat Steps 3 and 4 for other rules.

Managing Subscriber Notifications Overview

The subscriber notification feature pushes web-based messages to a subscriber by redirecting the subscriber HTTP traffic to relevant web pages. These web pages contain information relevant to the subscriber, such as notifications of quota depletion. HTTP redirection starts when the subscriber notification is activated and ceases when the notification is dismissed.

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

Each set of subscriber redirection parameters comprises a notification redirect profile. The Cisco SCA BB supports a maximum of 128 redirect profiles, including notification and redirect profiles. There are 3 default

redirect profiles that cannot be deleted: Default Notification, Network Attack Notification, and Default Redirection. You configure which notification redirect profile to use when defining rules.

Subscriber Notification Parameters

Each redirect profile of type notification contains the following subscriber notification parameters:

Note The Activation trigger configuration options are only available for redirect profile of type redirect.

- Name—Each profile must have a unique name.

Note You cannot change the name of the Default Notification or the Network Attack Notification.

- Redirect profile type—Each profile must be one of two types:
  - Notification
  - Redirect
- Set of Redirection URLs—A configurable set of destination URLs, to which the HTTP flows of the subscriber are redirected after redirection is activated. This web page usually contains the message that needs to be conveyed to the subscriber. The redirection set can optionally include one, or several parameters appended to the destination URL including the redirect reason and subscriber ID.

The destination web server can use these parameters to carry a more purposeful message to the subscriber.

- Activation frequency—Indicates when to activate the notification redirect. The activation frequency is one of the following:

Note The Periodically option is only available for redirect profile of type redirect.

- Only once—The subscriber is redirected to the notification only the first time the conditions are met.

For example, if a quota was exceeded, the subscriber browses to the destination URL that informs them of this fact, only once (even though the subscriber remains in a breach state).

- Always—The subscriber is redirected to the notification every time the conditions are met.

For example, if a quota was exceeded, the subscriber is continuously redirected to the notification until the subscriber completes the procedure to refresh their quota.

- Until the subscriber browses to—Every time the conditions are met, the subscriber is redirected to the notification, until the subscriber proceeds from the destination URL to a different, final URL.

For example, if a quota was exceeded, the web page at the destination URL may ask the subscriber to press an Acknowledge button after reading the message. The acknowledge URL would be defined as the dismissal URL and would deactivate further notifications.

The dismissal URL is composed of the URL hostname and the URL path, separated by a colon, in the following format:

[*]<hostname>:<path>[*]

- < hostname > may optionally be preceded by a wildcard (*), to match all hostnames with the same suffix.
- The path element must always start with "/".
- < path > may be followed by a wildcard (*), to match all paths with a common prefix.

For example, the entry *. some-isp.net:/redirect/ * matches all the following URLs:

- www.some-isp.net/redirect/index.html
- support.some-isp.net/redirect/info/warning.asp
- noquota.some-isp.net/redirect/acknowledge.aspx?ie=UTF-8

- List of Allowed URLs—A list of URLs that are not blocked and redirected even though redirection is activated.

After redirection is activated, all HTTP flows, except flows to the destination URL and to the dismissal URL, are blocked and redirected to the destination URL. However, subscribers can be permitted to access an additional set of URLs. This is useful, for example, to give subscribers access to additional support information.

Allowed URLs have the same format as the dismissal URL.

These parameters are defined when you add a new notification redirect profile (see Adding a Set of Redirection URLs, on page 430 section). You can modify them at any time.

- Once in a day—The subscriber is redirected only the first time when the conditions are met and this also happens the first time every day.
- Once in a week—The subscriber is redirected only the first time when the conditions are met and this also happens the first time every week.
- Once in a Month—The subscriber is redirected only the first time when the conditions are met and this also happens the first time every month.



Note By default "Across login " support is enabled for the above three options . Redirection History RDR will be generated every time , when the redirection condition is met . The Subscriber manager processes those RDRs and shares the redirected profile information on the next login The Redirection History RDR will be generated to reset the marked profiles, once at the end of a Day, a Week and a Month . By this way we are achieving the redirection only once in a Day , Week and Month .

For more information, see "Subscriber Redirection" section in Cisco Subscriber Manger user guide.

For more information, see "Redirection History RDR" section in *Cisco Service Control Application for Broadband reference guide* and see "Configuring the Subscriber Redirection Across Login" section in *Cisco SCE 10000 Software Configuration Guide*

Network Attack Notification

Subscriber notification informs a subscriber in real-time about current attacks involving IP addresses mapped to that subscriber. (Enabling these notifications is described in " The Service Security Dashboard .) Cisco SCA BB notifies the subscriber about the attack by redirecting HTTP flows originating from the subscriber to a server that supplies information about the attack.

One subscriber notification, Network Attack Notification, is dedicated to providing these notifications; it cannot be deleted. A Network Attack Notification is not dismissed at the end of an attack; subscribers must respond to it.

To allow redirection when blocking traffic, the system is configured to leave open one specified TCP port (by default, port 80). See "Advanced Service Configuration Options" section.

Note In earlier releases of Cisco SCA BB, configuring network attack notifications was performed using CLI commands. CLI commands should no longer be used for this purpose.

Network Attack Notification Parameters

When a network attack is detected, HTTP flows of the subscriber are redirected to a configurable destination URL. This web page should display the warning that needs to be conveyed to the subscriber.

Optionally, the destination URL can include a query part containing notification parameters. The destination web server can use these parameters to create a more specific warning to the subscriber.

The query part of the URL has the following format:



Table 11: Description Tail Fields

Field	Description	Possible Values
ip	Detected IP address	
side	—	• s—Subscriber • n—Network
dir	—	• s—Source • d—Destination
protocol	—	• TCP • UDP • ICMP • OTHER

Field	Description	Possible Values
open-flows	Number of open flows	—
suspected flows	Number of attack-suspected flows	—
open-flows-threshold	Threshold for open flows	—
suspected-flows-threshold	Threshold for attack-suspected flows	—
action	—	• R—Report • B—Block and report
handled-flows	Number of flows handled since the attack began (Non-zero only during and at the end of an attack)	—

Example of URL with Description Tail

http://www.some-isp.net/warning?ip=80.178.113.222&side=s&proto=TCP&no=34&nd=4&to=34&td=10&ac=B&nh=100

Adding a Notification Redirect Profile

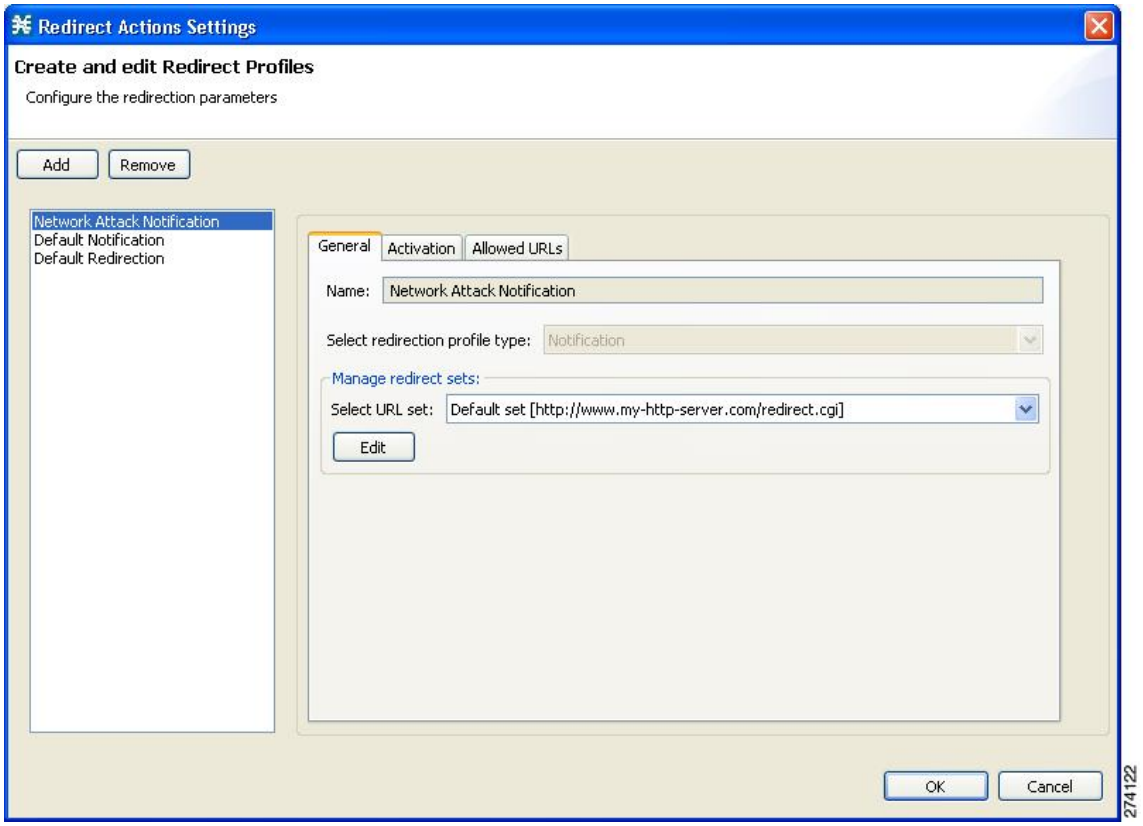
Note Creating a notification redirect profile does not activate the subscriber notification feature. After the notification redirect profile is defined, it must be activated for a particular package

Procedure

Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies** > **Subscriber Redirection**.

The Redirect Actions Settings dialog box appears.

Figure 292: Redirect Action Settings - General Tab



Step 2 Click **Add**.
A new redirection profile containing the default redirection URL set is added to the redirection profile list.

Step 3 In the Name field, enter a unique name for the new notification redirect profile.
You can use the default name for the notification redirect profile. It is recommended that you enter a meaningful name.

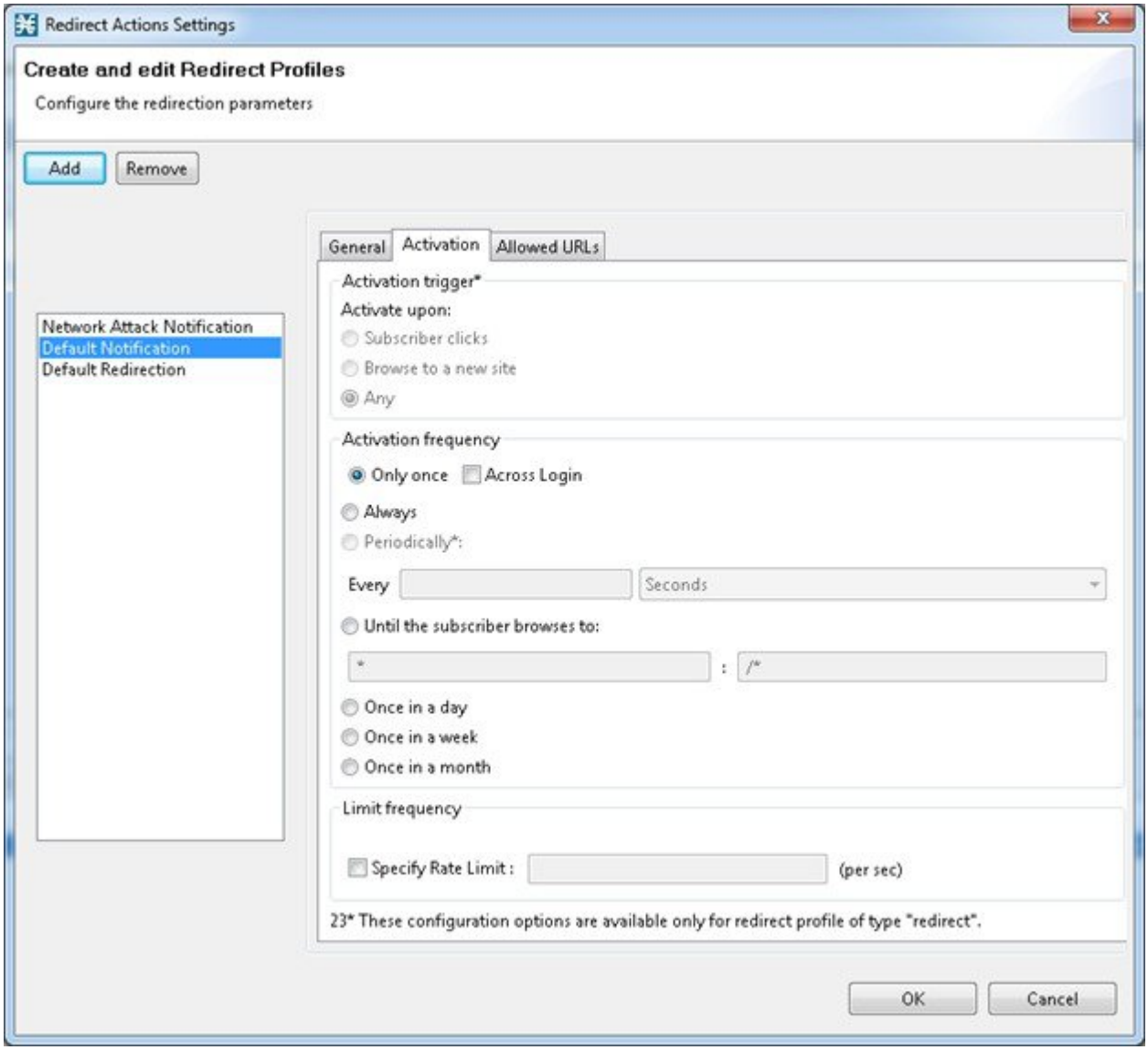
Step 4 In the Select redirection profile type field, select **Notification**.
Do not skip this step or a redirect profile is created instead of a notification redirect profile.

Step 5 Choose a URL set.

Step 6 Click the Activation tab.

The Activation tab opens.

Figure 293: Activation Tab



Step 7 Configure the frequency in which the redirection is triggered. Choose one of the Activation frequency radio buttons:

- Only once
- Always
- Until the subscriber browses to
- Once in a day
- Once in a week

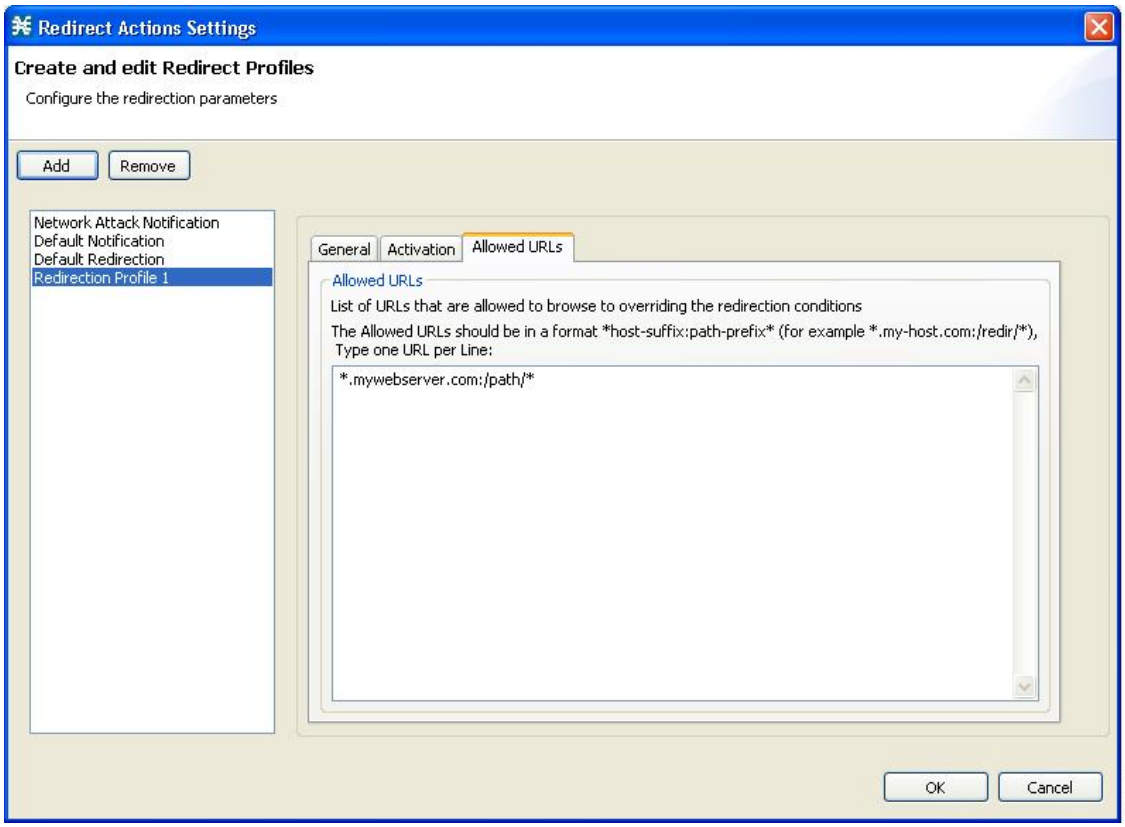
- Once in a month

Step 8 If you chose the Until the subscriber browses to: radio button, enter the dismissal URL host-suffix and path-prefix in the fields provided.

Note We recommend that you avoid configuring the same host for redirection URL and redirection dismissal URL. The redirection is done based on the first GET request in a flow. If the same host is configured, with the changes in the URL path, the GET request corresponding the dismissal URL may use the same flow that was created for the redirect URL. This is the expected behavior with the default configuration. You can change the default configuration by increasing the number of HTTP GET detections in the flow. To modify the number of HTTP GET detections from the Cisco SCA BB, use the Advanced Service Configuration Options. Note that increasing the number of HTTP GET detections may impact the performance of the Cisco SCE.

Step 9 Click the Allowed URLs tab.
The Allowed URLs tab opens.

Figure 294: Allowed URLs Tab



Step 10 Enter any allowed URLs, one per line.

Step 11 Click OK.
The Redirect Actions Settings dialog box closes.

The notification redirect profile is added to the profile list.

Managing Subscriber Redirection Overview

The rules for a package may deny access to selected protocols. When a subscriber to the package tries to access a blocked protocol, the traffic flow can be redirected to a server where a posted web page explains the reason for the redirection. For example, a "Silver" subscriber trying to access a service available only to "Gold" subscribers. This web page can offer subscribers the opportunity to upgrade their packages. You configure which redirection profile to use when defining rules.

Note Redirection is not supported when unidirectional classification is enabled.

Each redirect profile consists of a set of redirect parameters. The Cisco SCA BB supports a maximum of 128 redirect profiles, including notification redirect and redirect profiles.

Subscriber Redirect Parameters

Each redirect profile of type redirect contains the following parameters:

- Name—Each profile must have a unique name.

Note You cannot change the name of the Default Redirection Profile.

- Redirect profile type—Each profile must be one of two types:
  - Notification
  - Redirect
- Set of Redirection URLs—A configurable set of destination URLs, to which the subscriber's HTTP flows are redirected after redirection is activated. The redirection set can optionally include one, or several parameters appended to the destination URL including the redirect reason or subscriber ID.
- Activation trigger—The action that initiates the redirect. The activation trigger is one of the following:
  - Subscriber clicks—When the redirect is activated through a subscriber clicking a link.
  - Browse to a new site—When the redirect is activated through browsing.
  - Any—When the redirect is activated either via a link or browsing.
- Activation frequency—Indicates when to activate the redirect. The activation frequency is one of the following:
  - Only once—The subscriber is redirected only the first time the conditions are met. Enable the GT_GLB_RedirectOnHomePage tunable to redirect from a home page.
  - Always—The subscriber is redirected every time the conditions are met.
  - Periodically—The redirection is based on a periodic counter and the counter is reset after the redirection is complete.

- Triggering events
- KBytes
- Until the subscriber browses to—Every time the conditions are met, the subscriber is redirected, until the subscriber proceeds from the destination URL to a different, final URL.

The dismissal URL is composed of the URL hostname and the URL path, separated by a colon, in the following format:[*]<hostname>:<path>[*]

- < hostname > may optionally be preceded by a wildcard (*), to match all hostnames with the same suffix.
- The path element must always start with "/".
- < path > may be followed by a wildcard (*), to match all paths with a common prefix.

For example, the entry *. some-isp.net:/redirect /* matches all the following URLs:

- www.some-isp.net/redirect/index.html
- support.some-isp.net/redirect/info/warning.asp
- noquota.some-isp.net/redirect/acknowledge.aspx?ie=UTF-8

- List of Allowed URLs—A list of URLs that are not blocked and redirected even though redirection is activated.

After redirection is activated, all HTTP flows, except flows to the destination URL and to the dismissal URL, are blocked and redirected to the destination URL. However, subscribers can be permitted to access an additional set of URLs. This is useful, for example, to give subscribers access to additional support information.

Allowed URLs have the same format as the dismissal URL. But, for Allowed URLs, you must specify the HTTP port and the port must be 80. If the URL contains any port other than 80, the URL is considered as a normal URL and is redirected.

These parameters are defined when you add a new notification redirect profile. You can modify them at any time.

- Once in a day—The subscriber is redirected only the first time when the conditions are met and this also happens the first time every day.
- Once in a week—The subscriber is redirected only the first time when the conditions are met and this also happens the first time every week.
- Once in a Month—The subscriber is redirected only the first time when the conditions are met and this also happens the first time every month.



Note By default "Across login " support is enabled for the above three options . Redirection History RDR will be generated every time , when the redirection condition is met . The Subscriber manager processes those RDRs and shares the redirected profile information on the next login The Redirection History RDR will be generated to reset the marked profiles, once at the end of a Day, a Week and a Month . By this way we are achieving the redirection only once in a Day , Week and Month .

Note when the Subscriber Manger is configured in PUSH MODE, "once in a Day , a Week and a month" features are not supported.

- Limit Frequency—Used to rate limit the number of redirections occuring per second for this redirection profile. Remaining flows will be redirect to the next new flow.

For more information, see "Subscriber Redirection" section in Cisco Subscriber Manger user guide.

For more information, see "Redirection History RDR" section in *Cisco Service Control Application for Broadband reference guide* and see "Configuring the Subscriber Redirection Across Login" section in *Cisco SCE 8000 Software Configuration Guide*

Adding a Redirect Profile

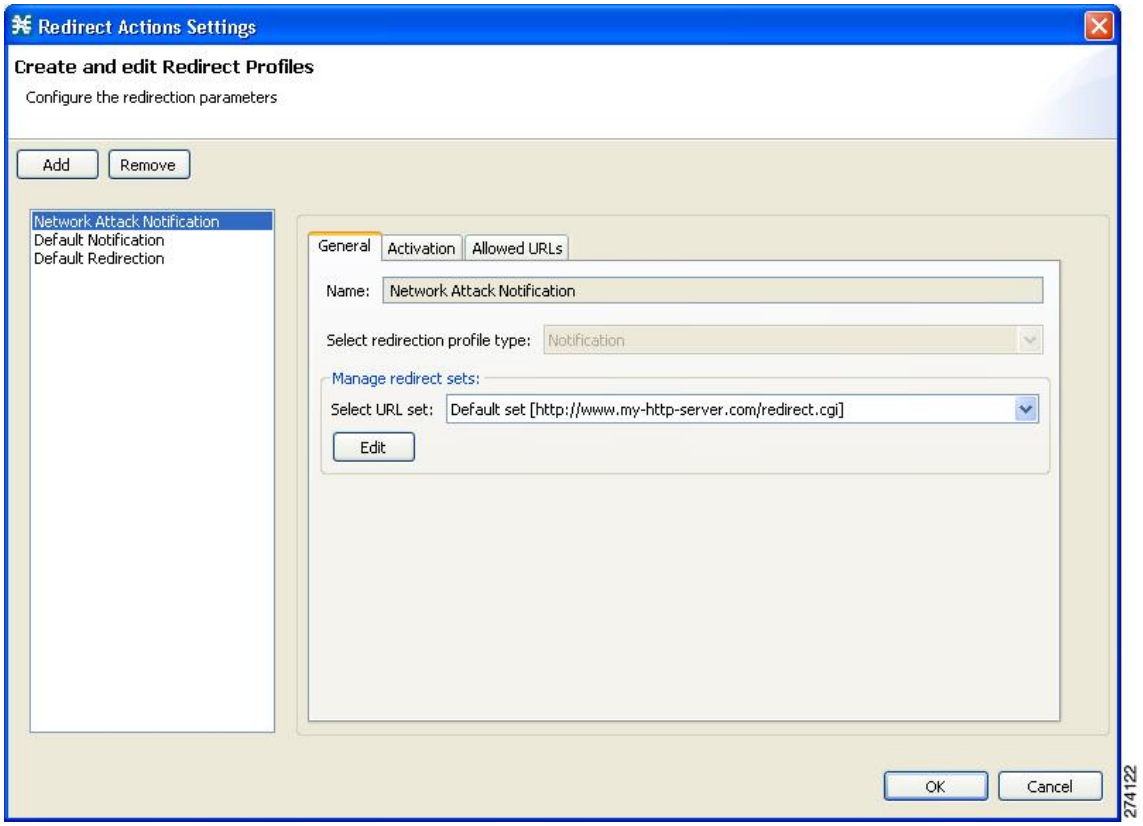
A redirect profile contains a set of redirection URLs as well as conditions in which to use the redirect feature, such as the action that triggers the redirect, or the frequency in which the redirect occurs.

Procedure

Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies** > **Subscriber Redirection**.

The Redirect Actions Settings dialog box appears.

Figure 295: Redirect Actions Settings - General Tab



Step 2 Click Add.
A new redirect profile containing the default redirection URL set is added to the redirect profile list.

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

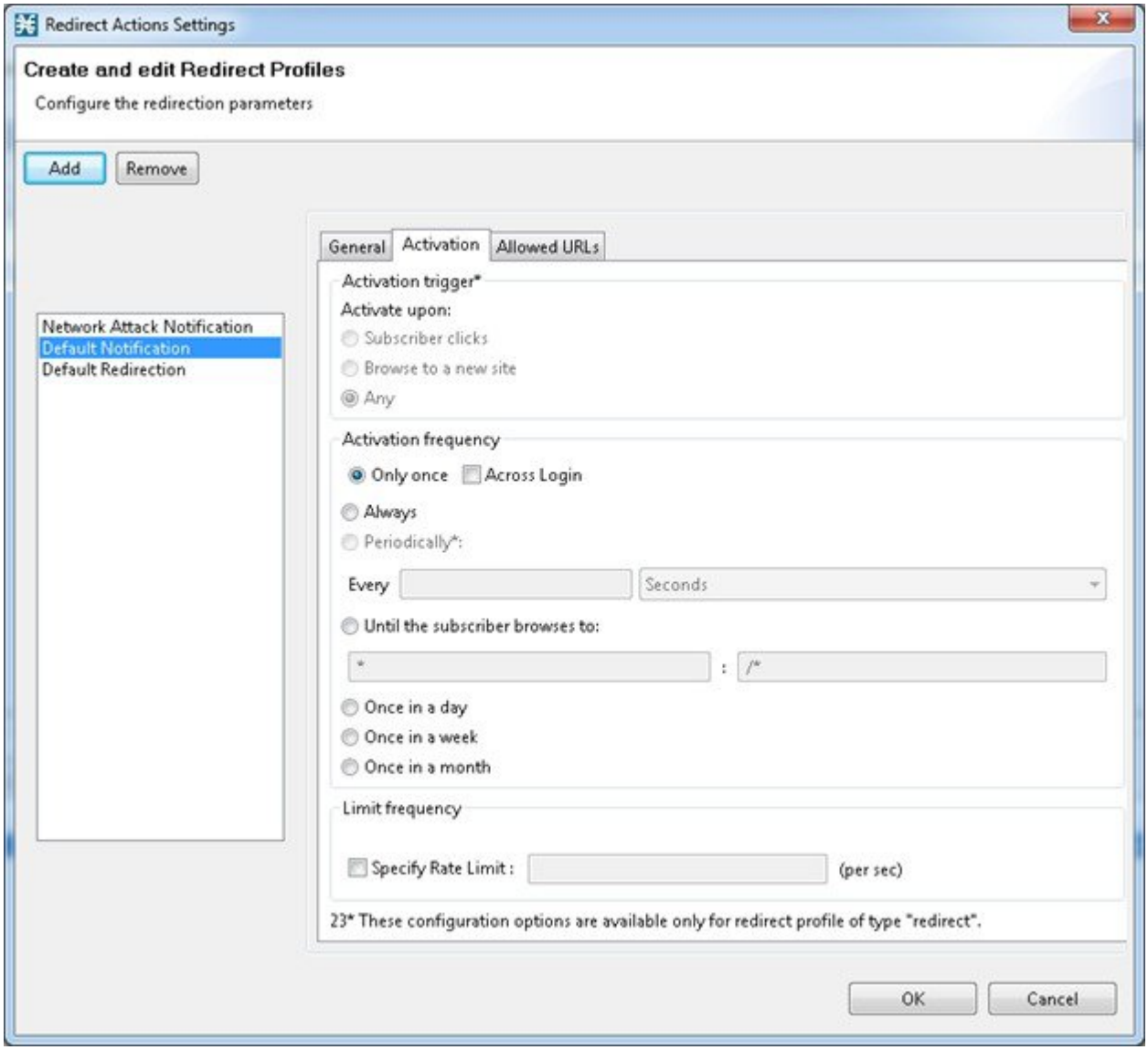
Note You can use the default name for the redirect profile, but it is recommended that you enter a meaningful name.

Step 4 Choose a URL set.

Step 5 Click the Activation tab.

The Activation tab opens.

Figure 296: Activation Tab



Step 6 Configure the activity that triggers the redirection. Choose one of the Activation trigger radio buttons:

- Subscriber clicks
- Browse to a new site
- Any

Step 7 To configure the frequency in which the redirection is triggered, choose one of the following activation frequency radio buttons:

- Only once
- Always
- Until the subscriber browses to
- Once in a day
- Once in a week
- Once in a month

Step 8 If you selected the Periodically radio button, enter a number and an increment in the Every fields, to specify the frequency in which the redirection occurs.

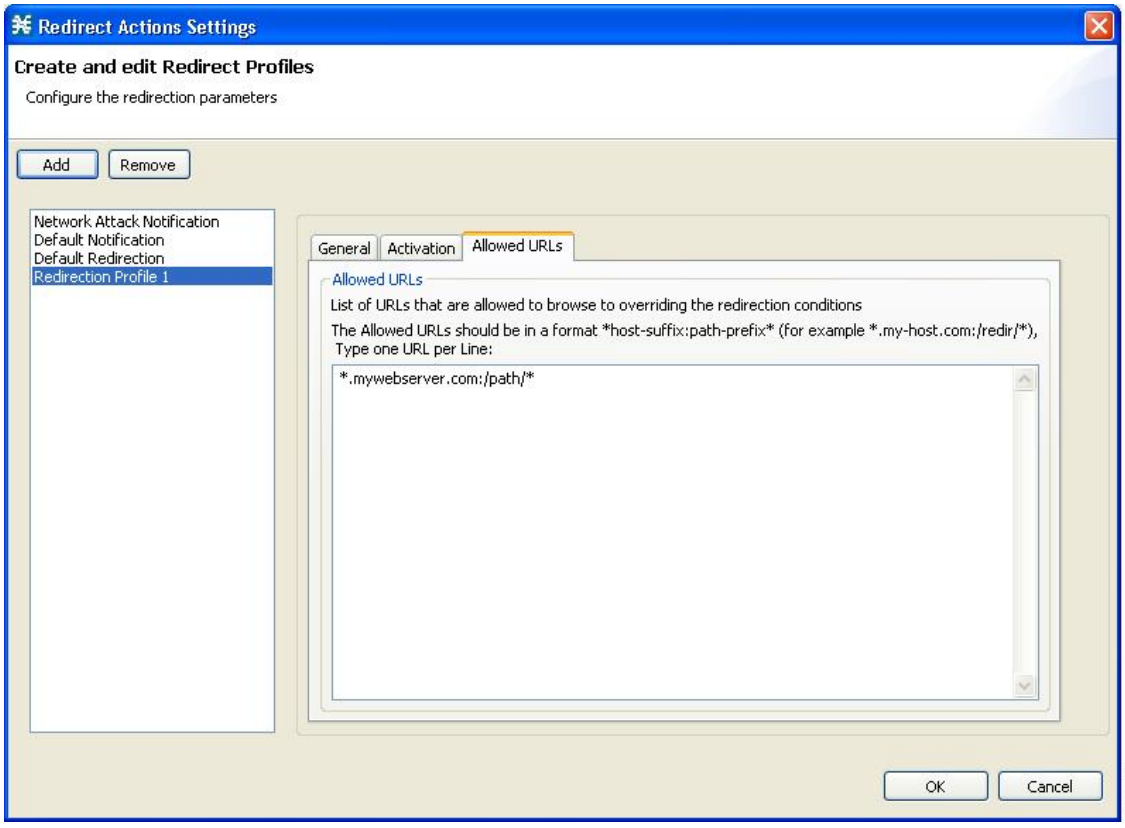
Step 9 If you selected the Until the subscriber browses to: radio button, enter the dismissal URL in the fields provided.

Step 10 Click the Allowed URLs tab.

Note Enter all configured redirection URLs to the Allowed URLs list to prevent a redirection loop.

The Allowed URLs tab opens.

Figure 297: Allowed URLs Tab



Step 11 Enter a URL, or multiple URLs (with HTTP port 80), that can be browsed, overriding the redirect conditions.

Note All URLs with HTTP port other than 80 is redirected.

Step 12 Click OK.

The Redirect Actions Settings dialog box closes.

The Redirection profile is added to the redirection profile list.

Deleting a Redirection Profile

You cannot delete the Default Redirection Profile.

Procedure

Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies** > **Subscriber Redirection**.
The Redirect Actions Settings dialog box appears.

Step 2 Click the name of the profile.

Step 3 Click **Remove**.

Step 4 Click **OK**.
The Redirect Actions Settings dialog box closes.

The Redirection settings are saved.

Adding a Set of Redirection URLs

The Console Redirection feature supports only three protocols:

- HTTP Browsing
- HTTP Streaming
- RTSP Streaming

Each redirection set contains one redirection option for each of these three protocols. The system provides a default redirection set, which cannot be deleted. You can add up to 127 additional sets.

Each redirection URL includes the URL specified name, the Subscriber ID, and the Service ID in the following format:

```
<URL>?n=<subscriber-ID>&s=<service-ID>
```

Optionally, the URL can contain one or multiple parameters appended to it.

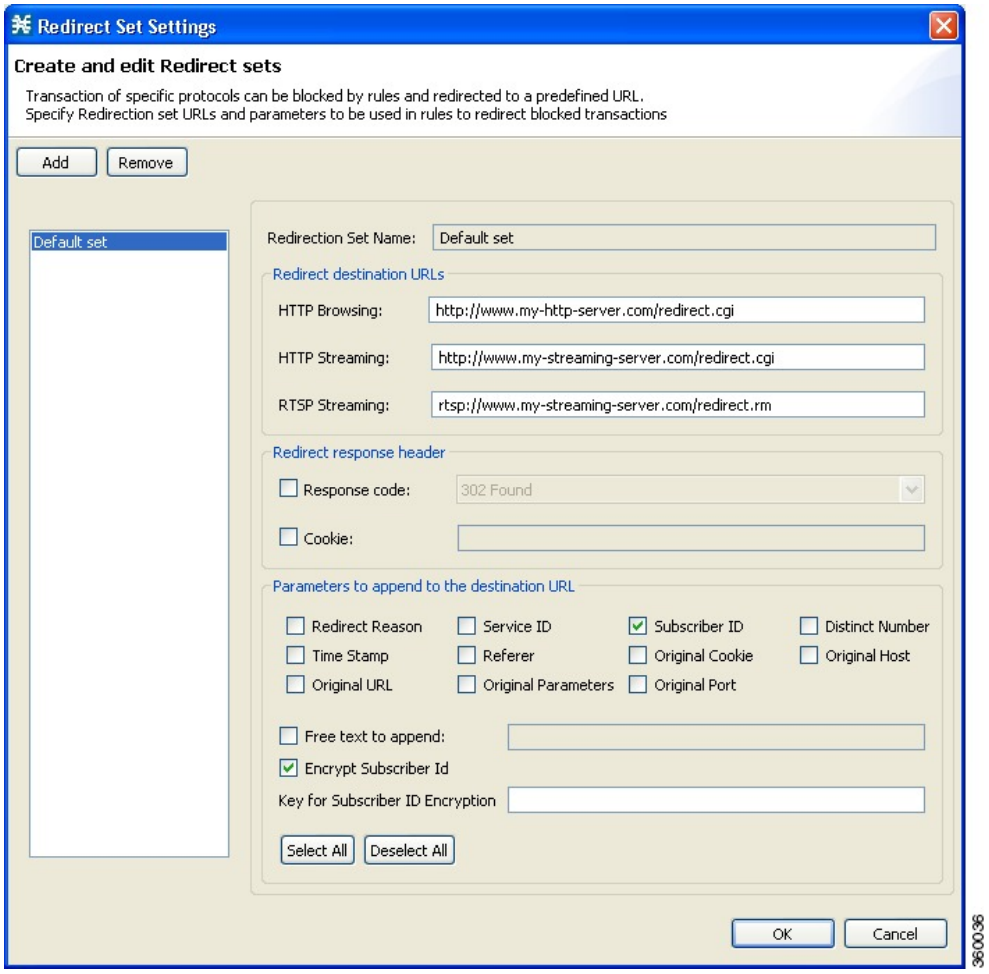
Procedure

Step 1 From the Policies tab of the left pane, choose **Configuration** > **Policies** > **Subscriber Redirection**.
The Redirect Actions Settings dialog box appears.

Step 2 In the General tab, click Edit.

The Redirect Set Settings dialog box appears.

Figure 298: Redirect Set Settings



Step 3 Click Add.
A new redirection set containing the default redirection URLs is added.

Step 4 In the Redirection Set Name field, enter unique name for the new redirection set.

Note You can use the default name for the redirection set, but it is recommended that you provide a meaningful name.

Step 5 Enter new values in the Redirection destination URLs section of the new redirection set.

Note Enter all configured redirection URLs to the Allowed URLs list to prevent a redirection loop.

Step 6 To include a response code, check the Response code check box, and choose a response code from the drop-down list. see Table 10-2 for a listing and description of the redirection parameters.

Step 7 To include a cookie, check the Cookie check box, and enter a value. see Table for a listing and description of the redirection parameters.

Step 8 Check the check boxes of any parameters you wish to append to the destination URL see Table for a listing and description of the redirection parameters.

If you check the Free text to append check box, enter text into the text box to append to the URL. see Table 10-2 for a listing and description of the redirection parameters. The examples in Table is based on the following URL redirection:

http:// <*URL*> ?n=N/A&reason=2&s=119&id=0:10&ts=1327285422&str=this is free text to append content&referer=&cookie=&host= <*URL*> &url=/p-cube.htm&params=

Note "<" and ">" do not appear in redirect URL. Maximum length of destination URL including parameters is 500 characters. Cookie and Referer parameters are allowed only for HTTP traffic.

Table 12: Redirection Parameters

Parameter	Description	Example
Redirect Reason	In case of notification—notification number. In case of DDOS attack—DDOS attack ID. In case of redirect—not valid.	2
Service ID	The ID of the service as was classified by the Cisco SCE.	119
Subscriber ID	Subscriber name as it appears in Cisco SCE.	—
Distinct Number	Unique identifier of redirected flow, in format <redirected flow number:cpu number>.	0:10
Time Stamp	Time in seconds, in UNIX format.	1327285422
Referer	Referer as it appears in the original flow request. If the referer parameter is not set then "" appears.	—
Original Cookie	Cookie string as it appears in the original flow request. If the cookie parameter is not set then "" appears.	—
Original Host	Host name as it appears in the original flow request.	<*URL*>
Original URL	URL as it appears in the original flow request.	/p-cube.htm
Original Parameters	URL parameters as they appear in the original flow request. If the URL parameters are not set then "" appears.	—

Parameter	Description	Example
Original Port	Server port number that is added to the redirect host parameter.	—
Free text to append	Free text.	this is free text to append content
Key for Subscriber ID Encryption	A 32-character hexadecimal encryption key to be entered in the Key for Subscriber ID Encryption field. The key must contain 32 hexadecimal characters.	770A8A65DA156D24EE2A093277530142

Step 9 Click OK.

Your settings are saved and the Redirect Set Settings dialog box closes.



Note Keep the total number of characters appended to the redirect URL below 1200. To keep it below 1200, we recommend that you enable only the required parameters under the Parameters to append to the destination URL pane.

Deleting a Set of Redirection URLs

Procedure

Step 1 From the Policies tab of the left pane, choose **Configuration** > **Policies** > **Subscriber Redirection**.
The Redirect Actions Settings dialog box appears.

Step 2 In the General tab, click **Edit**.
The Redirect Set Settings dialog box appears.

Step 3 Click the name of the redirection set.

Step 4 Click **Remove** .

Step 5 Click **OK**.
The Redirect Set Settings dialog box closes.

The Redirection settings are saved.

Managing the System Settings Overview

The Console allows you to determine various system parameters that control:

System Operational Mode

The operational mode of the system defines how the system handles network traffic.

Note Each rule has its own operational mode (state). If this differs from the system mode, the "lower" of the two modes is used. For example, if a rule is enabled, but the system mode is report-only, the rule generates only RDRs.

The three operational modes are:

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

Setting the Operational and Topological Modes of the System

Asymmetric Routing Classification Mode

Enabling unidirectional classification significantly improves classification accuracy when the Cisco SCE platform is deployed in an environment with a high rate of unidirectional flows.

Unsupported Features

The following Cisco SCA BB features are not supported when unidirectional classification is enabled:

- Flavors
- External quota provisioning
- Subscriber notification
- Redirection
- Flow Signaling RDRs
- Content filtering
- VAS traffic forwarding

When unidirectional classification is enabled, the service configuration editor indicates (in the Problems View) if the service configuration is consistent with the features that are supported in this mode.

The following features, which are not part of the service configuration, are also affected when unidirectional classification is enabled:

- Subscriber-Aware Mode (a mode in which subscriber information is dynamically bound to the IP address currently in use by the subscriber) is not supported.
- Enhanced flow open mode must be enabled.

The system gives no indication if the state of the above features is consistent with the state of the routing classification mode.

Protocol Classification

When unidirectional classification is enabled, protocol classification is performed in the normal way except for unidirectional UDP flows. Because it is impossible to know the server side of a unidirectional UDP flow, Cisco SCA BB tries to classify the protocol using the destination port of the first packet; if no exact match is found, Cisco SCA BB tries to classify the protocol using the source port.

Switching to Asymmetric Routing Classification Mode

If you create a service configuration in symmetric mode and switch to asymmetric routing classification mode:

- Flavors are not used for classification.
- Periodic quota management mode is used.
- Data is not lost when you switch to asymmetric routing classification mode, but you cannot apply the service configuration to a Cisco SCE platform until all unsupported features are removed from the service configuration.

Switching from Asymmetric Routing Classification Mode

If you create a service configuration in asymmetric routing classification mode:

- The Suspected Session Rate is set equal to the Session Rate for all anomaly detectors.
- No flavors are created in the default service configuration, and no service elements have specified flavors.
- The quota management mode is periodic, with a daily aggregation period.
- Asymmetric routing classification mode limitations remain if you switch to symmetric mode. To change them, you must edit the service configuration.

Advanced Service Configuration Options

Advanced service configuration options control the more sophisticated and less frequently changed attributes of the system. It is recommended that you do not change these options.

The Advanced Service Configuration Properties

Table 13: Advanced Service Configuration Properties

Property	Default Value	Description
Add On Package		
Enable Add On Package	FALSE	Enables addition of the Add On Packages
Bandwidth Management		
Level of BWC enforcement on networking flows of P2P and IM applications.	SCE to use Default Service BWCs.	Specifies the level of BWC enforcement on networking flows of P2P and IM applications.

Property	Default Value	Description
Use Global Bandwidth Management in Virtual Links Mode	FALSE	Specifies whether to use the Global Bandwidth Management in Virtual Links Mode.
Classification		
Apply this order of priority between different criteria for service classification	Zone > Flavor > Protocol > Init-Side	Specifies the order of priority between different criteria for service classification. Values are: • Flavor > Protocol > Zone > Init-Side • Zone > Flavor > Protocol > Init-Side
ClickStream Event recognition	TRUE	Specifies whether to recognize ClickStream Events.
Enable sending '404, Page Not Found' upon blocking	FALSE	Specifies whether to send '404, Page Not Found' upon blocking.
Guruguru detailed inspection mode enabled	FALSE	The Guruguru protocol is used by the Guruguru file-sharing application popular in Japan. Cisco SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little Guruguru traffic is expected. This mode is usual in all countries except Japan. • Detailed—Suitable for networks where Guruguru traffic is expected to be common. This mode is used in Japanese networks only.
Kuro detailed inspection mode enabled	FALSE	The Kuro protocol is used by the Kuro file-sharing application popular in Japan. Cisco SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little Kuro traffic is expected. This is usual in all countries except Japan. • Detailed—Suitable for networks where Kuro traffic is expected to be common. This mode is used in Japanese networks only.

Property	Default Value	Description
Number of HTTP GET detections	1	Specifies the number of HTTP GET detections. The Cisco SCE classifies the HTTP based on the number of GET requests configured. Range is 1 to 65535, and the default value is 1. **Note** Since the Deep HTTP Inspection feature examines all packets in a single HTTP stream until the configured number of requests has been found, any value higher than 1 may impact the performance of the Cisco SCE.
Soribada detailed inspection mode enabled	FALSE	The Soribada protocol is used by the Soribada file-sharing application popular in Japan. Cisco SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little Soribada traffic is expected. This is usual in all countries except Japan. • Detailed—Suitable for networks where Soribada traffic is expected to be common. This mode is used in Japanese networks only.
TCP destination port signatures	1720:H323	TCP destination port numbers for signatures that require a port hint for correct classification. Valid values are comma-separated items, each item in the form <port-number>:<signature-name>. Applicable signature names are: H323, Radius Access, Radius Accounting, and DHCP.

Property	Default Value	Description
UDP destination port signatures	67:DHCP, 68:DHCP, 1812:Radius Access, 1645:Radius Access, 1813:Radius Accounting, 1646:Radius Accounting	UDP destination port numbers for signatures that require a port hint for correct classification. Valid values are comma-separated items, each item in the form <port-number>:<signature-name>. Applicable signature names are: H323, Radius Access, Radius Accounting, and DHCP.
UDP ports for which flow should be opened on the first IPv6 packet	5060, 5061, 69, 546, 547, 2427, 2727, 9201, 9200, 123, 1900, 5190, 10000	
UDP ports for which flow should be opened on the first packet	5060, 5061, 67, 68, 69, 1812, 1813, 1645, 1646, 2427, 2727, 9201, 9200, 123, 1900, 5190, 10000	
UDP source port signatures	1812:Radius Access, 1645:Radius Access, 1813:Radius Accounting, 1646:Radius Accounting	UDP source port numbers for signatures that require a port hint for correct classification. Valid values are comma-separated items, each item in the form <port-number>:<signature-name>. Applicable signature names are: H323, Radius Access, Radius Accounting, and DHCP.
V-Share detailed inspection mode enabled	FALSE	The V-Share protocol is used by the V-Share file-sharing application popular in Japan. Cisco SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little V-Share traffic is expected. This mode is usual in all countries except Japan. • Detailed—Suitable for networks where V-Share traffic is expected to be common. This mode is used in Japanese networks only.

Property	Default Value	Description
Winny detailed inspection mode enabled	FALSE	The Winny P2P protocol is used by the Winny file-sharing application popular in Japan. Cisco SCA BB provides two inspection modes for classification of this protocol: • Default—Suitable for networks where little Winny traffic is expected. This is usual in all countries except Japan. • Detailed—Suitable for networks where Winny traffic is expected to be common. This mode is used in Japanese networks only.
WinnyP aggressive classification enabled	FALSE	—
WinnyP classification enabled	FALSE	—
Malicious Traffic		
Malicious Traffic RDRs enabled	TRUE	Specifies whether to generate Malicious Traffic RDRs.
Number of seconds between Malicious Traffic RDRs on the same attack	60	A Malicious Traffic RDR is generated when an attack is detected. Malicious Traffic RDRs are then generated periodically, at user-configured intervals, for the duration of the attack.
TCP port that should remain open for Subscriber Notification	80	You can choose to block flows that are part of any detected network attack, but this may hinder subscriber notification of the attack. The specified TCP port is not blocked to allow notification of the attack to be sent to the subscriber.
Multi Stage Classification		
Blocking	FALSE	Specifies whether to block the sub services under the main service.

Property	Default Value	Description
Enable	TRUE	Specifies whether to enable the sub service classification of a service. Multi stage classification describes the application level services that can be enabled or disabled. By default sub service classification of the services is enabled. For example, Google talk service contains Google talk file transfer, Google talk Networking, Google talk VoIP as sub services.
Policy Check		
Ongoing policy check mode enabled	TRUE	Specifies whether policy changes affect flows that are already open.
Time to bypass between policy checks (seconds)	30	Maximum time (in seconds) that may pass before policy changes affect flows that are already open.
Quota Management		
Grace period before first breach (seconds)	2	The time (in seconds) to wait after a quota limit is breached before the breach action is performed. Policy servers should use this period to provision quota to a subscriber that just logged in.
Length of the time frame for quota replenish scatter (minutes)	0	The size of the window across which to scatter the periodic quota replenishment randomly.
Time to bypass between policy checks for quota limited flows	30	Maximum time (in seconds) that may pass before a quota breach affects flows that are already open.
Volume to bypass between policy checks for quota limited flows	0	Maximum flow volume (in bytes) that may pass before a quota breach affects flows that are already open. A value of zero means that unlimited volume may pass.
Redirection		
Adds original host to redirection URL	FALSE	Specifies whether to add the original host to the redirection URL.

Property	Default Value	Description
Adds original URL to redirect URL	FALSE	Specifies whether to add the original URL to the redirection URL.
Maximum redirect URL Length	500	Specifies the maximum length of the redirect URL.
Redirect subscriber ID format	Complete - n=<user>@<realm>	Specifies the redirect subscriber ID format to be configured. Valid Options are: • Complete - n=<user>@<realm> (default) • User only - n=<user> • Realm only - r=<realm> • Separately -n<user>&r=<realm> If the subscriber name does not match the format of <user>@<realm>, the full subscriber name is appended to the URL, regardless of the redirect subscriber format configured.
Reporting		
Extract Full User Agent details	FALSE	Specifies whether to extract full user agent details.
Flow Accounting RDRs enabled	FALSE	Specifies whether to generate Flow Accounting RDRs.
Flow Accounting RDRs interval for each Service (in seconds)	60	Specifies the interval at which the Flow Accounting RDRs are generated for each service.
Flow Accounting RDRs limit per second	100	Specifies the limit of Flow Accounting RDRs to be generated each second.

Property	Default Value	Description
Hide Subscriber IP and ID in RDRs	FALSE	Specifies whether to hide the IP address and Subscriber ID in the following RDRs: • Transaction RDR • Transaction Usage RDR • HTTP Transaction Usage RDR • RTSP Transaction Usage RDR • VoIP Transaction Usage RDR • Video Transaction Usage RDR • Blocking RDR • Flow Start RDR • Flow End RDR • Flow Ongoing RDR • Media Flow RDR • Spam RDR See the Cisco Service Control for Broadband Reference Guide for details on the RDRs.
Hide Subscriber IP and ID in RDRs with Empty String	FALSE	Specifies whether to nullify subscriber IP address and Subscriber ID when Anonymize RDR support is enabled.
Media Flow RDRs enabled	TRUE	Specifies whether to generate Media Flow RDRs.
Minimal volume for generating HTTP Transaction Usage RDR (bytes)	0	Specifies the minimum volume for generating HTTP Transaction Usage RDR.
Minimal volume for generating RTSP Transaction Usage RDR (bytes)	0	Specifies the minimum volume for generating RTSP Transaction Usage RDR.
Minimal volume for generating Video Transaction Usage RDR (bytes)	1024000	Specifies the minimum volume for generating Video Transaction Usage RDRs.
Video Transaction Usage RDRs enabled	TRUE	Specifies whether to generate Video Transaction Usage RDRs.
Enable VSA Fields for Subscriber, HTTP Transaction, and Video Transaction RDRs	FALSE	Specifies whether to generate VSA fields for Subscriber, HTTP Transaction, and Video Transaction RDRs.

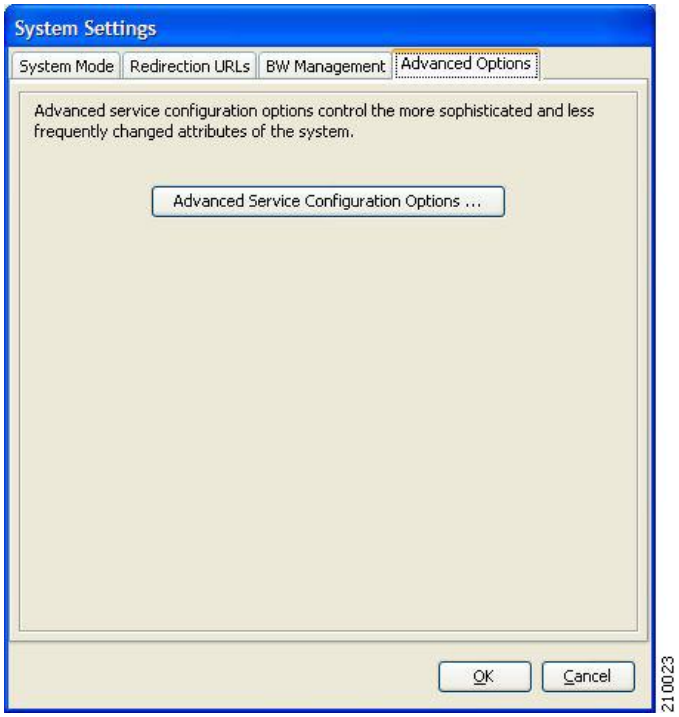
Editing Advanced Service Configuration Options

Procedure

Step 1 From the Policies tab of the left pane, choose Configuration > Policies > System Settings .

Step 2 Click the Advanced Options tab.
The Advanced Options tab opens.

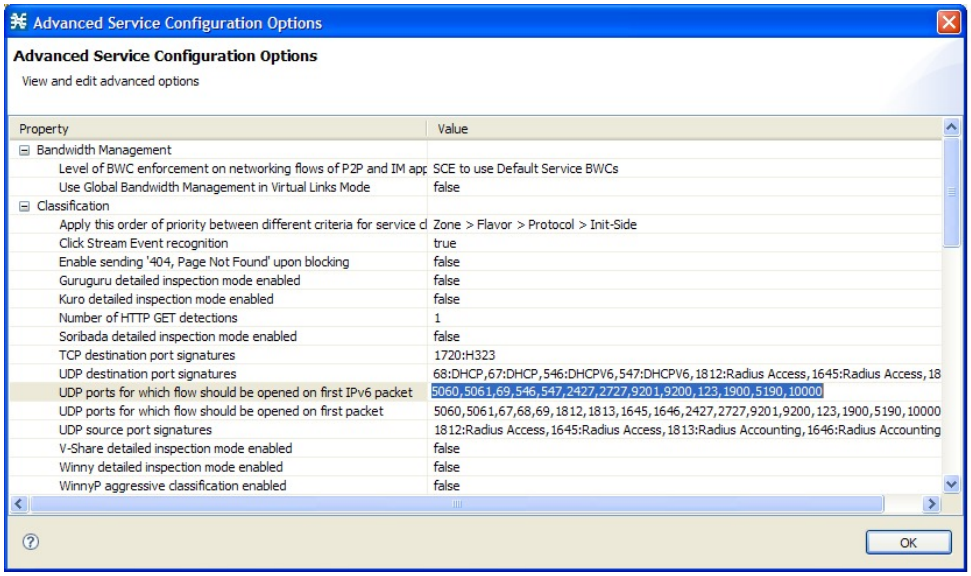
Figure 299: Advanced Options Tab



Step 3 Click Advanced Service Configuration Options .

The Advanced Service Configuration Options dialog box opens.

Figure 300: Advanced Service Configuration Options



Step 4 Make your changes to the configuration options.

Step 5 Click OK .
The Advanced Service Configuration Options dialog box closes.

The changes to the advanced options are saved.

Step 6 Click OK .
The System Settings dialog box closes.

Managing VAS Settings Overview

Value Added Service (VAS) settings includes the following features:

- Traffic mirroring—Traffic mirroring allows using the Cisco SCE to mirror a portion of the traffic based on its application and subscriber awareness. Traffic to be mirrored continues forwarding as is, and copies of the packets are sent to the corresponding VAS VLAN, thereby minimizing traffic.
- Traffic forwarding—Traffic forwarding servers allows you to use an external expert system (VAS server) for additional traffic processing, such as intrusion detection and content filtering to subscribers. After processing, flows are sent back to the Cisco SCE platform, which then sends them to their original destinations.

The flows to be forwarded are selected based on the subscriber package and the flow type (IP protocol type and destination port number).

VAS mirroring has the following limitations:

- The support traffic mirroring.
- Traffic mirroring is supported on any Cisco SCE platform that has at least 2 ports.

VAS forwarding has the following limitations:

- Only the platforms support VAS traffic forwarding.
- A single Cisco SCE platform can support up to eight VAS servers.
- A service configuration can contain up to 64 traffic-forwarding tables.
- A traffic-forwarding table can contain up to 64 table parameters.
- VAS traffic forwarding is not supported when unidirectional classification is enabled.



Note Because of the complexity of the VAS settings features, VAS flows are not subject to global bandwidth control.

To use VAS traffic forwarding:

- You must configure VAS services on the Cisco SCE platform.
- You must also assign the VAS traffic-forwarding tables to packages in the Advanced tab of the Edit Packages dialog. VAS traffic-forwarding is based on per-package configuration of where to forward what traffic.

Enabling VAS Traffic Forwarding

By default, VAS traffic forwarding is disabled. You can enable it at any time.



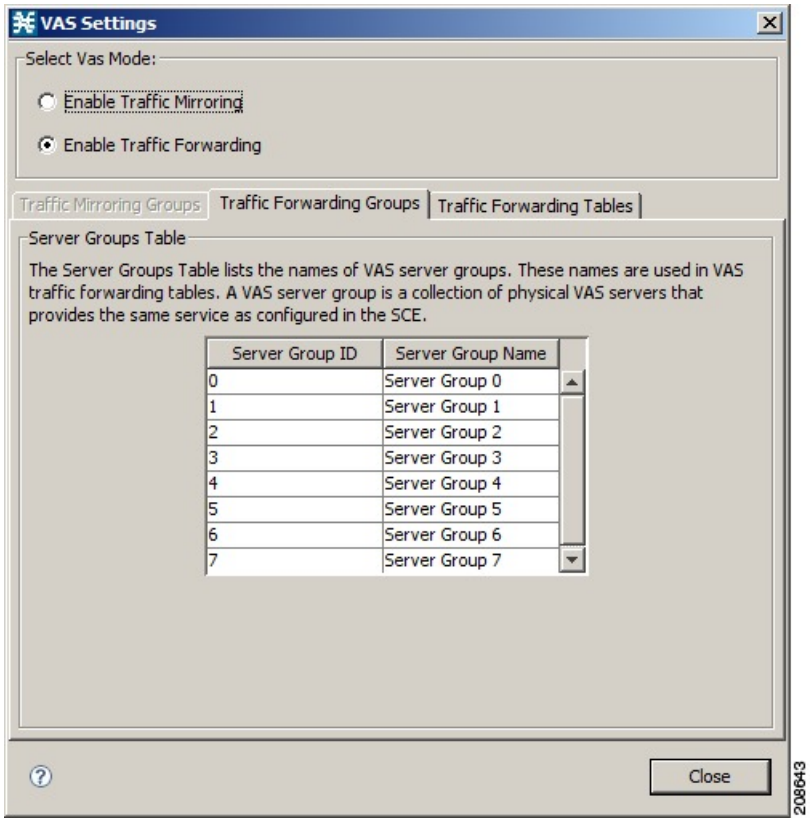
Note VAS traffic forwarding is not supported when unidirectional classification is enabled.

Procedure

Step 1 From the Policies tab of the left pane, choose **Configuration** > **Policies** > **VAS Settings**.

The VAS Settings dialog box appears.

Figure 301: VAS Settings - Enable Traffic Forwarding



Step 2 Click the Enable Traffic Forwarding radio button.
A VAS warning message appears.

Step 3 Click **OK**.

Step 4 Click **Close**.
The VAS Settings dialog box closes.

Enabling VAS Traffic Mirroring

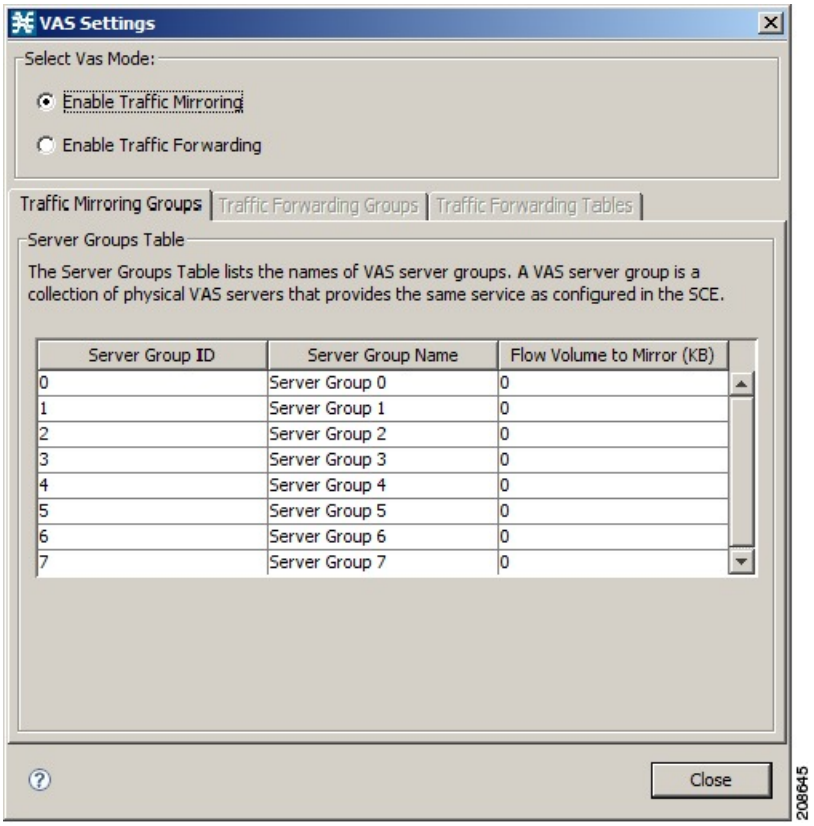
Traffic Mirroring in enabled and configured in the VAS Setting dialog box. However, you configure which server group to use when defining rules.

Procedure

Step 1 From the Policies tab of the left pane, choose **Configuration** > **Policies** > **VAS Settings**.

The VAS Settings dialog box appears.

Figure 302: VAS Settings - Enable Traffic Mirroring



Step 2 Choose the **Enable Traffic Mirroring** radio button.
A VAS warning message appears.

Step 3 Click **OK**.

Step 4 Click **Close**.
The VAS Settings dialog box closes.

Renaming VAS Server Groups

A Cisco SCE platform can forward flows to up to eight different VAS server groups. By default, the eight server groups are named “Server Group n”, where n takes a value from 0 to 7. Give the server groups meaningful names; the names you give appears in the drop-down list in the Control and Breach Handling tabs of the Add Rule to Package dialog box (see “How to Set Advanced Package Options” section) and in the Server Group field of the table parameters added to each traffic-forwarding table (see “Managing VAS Table Parameters” section).

Procedure

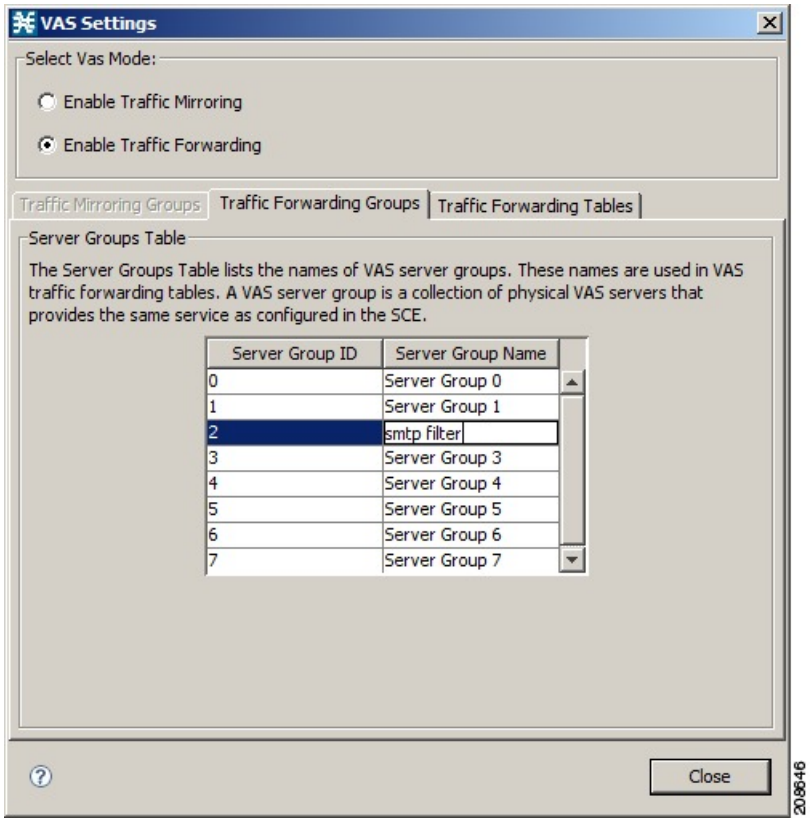
Step 1 From the Policies tab of the left pane, choose Configuration > Policies > VAS Settings .
The VAS Settings dialog box appears.

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 Step 2 and Step 3 for other server groups you wish to rename.

Figure 303: Traffic Forwarding Groups Tab



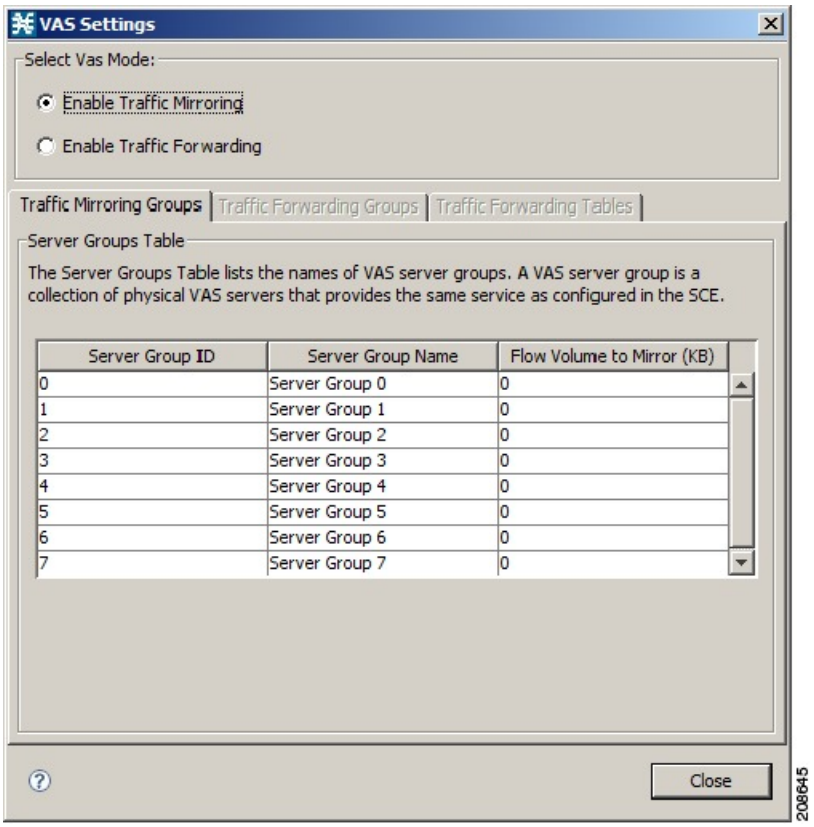
Step 5 Click Close .
The VAS Settings dialog box closes.

Configuring VAS Traffic-Mirroring

Procedure

Step 1 From the Policies tab of the left pane, choose Configuration > Policies > VAS Settings.
The VAS Settings dialog box appears.

Figure 304: Traffic Mirroring Groups Tab



Step 2 Click the Enable Traffic Forwarding radio button.

Step 3 For each server group, in the Flow Volume to Mirror (KB) column, enter the maximum amount of volume to mirror, in KB.

Step 4 Click Close .
The VAS Settings dialog box closes.

Viewing VAS Traffic-Forwarding Tables

Cisco SCA BB decides whether a flow passing through a Cisco 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.

Procedure

Step 1 From the Policies tab of the left pane, choose **Configuration** > **Policies** > **VAS Settings**.
The VAS Settings dialog box appears.

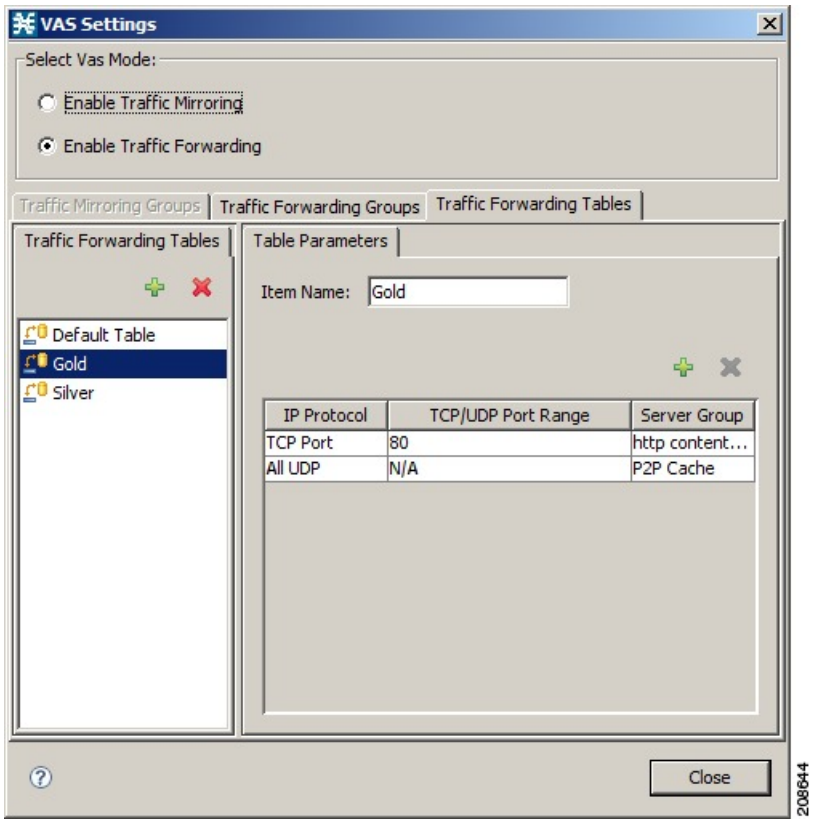
Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 Click the **Traffic Forwarding Tables** tab.
The Traffic Forwarding Tables tab opens.

A list of all traffic-forwarding tables is displayed in the Traffic Forwarding Tables area.

Step 4 Click a table in the list of traffic-forwarding tables to display its table parameters.
A list of all table parameters defined for this traffic-forwarding table opens in the Table Parameters tab.

Figure 305: Traffic Forwarding Tables Tab



Step 5 Click Close .

The VAS Settings dialog box closes.

Deleting VAS Traffic-Forwarding Tables

You can delete all user-created traffic-forwarding tables. The default traffic-forwarding table cannot be deleted.

Note A traffic-forwarding table cannot be deleted while it is associated with a package.

Procedure

Step 1 From the Policies tab of the left pane, choose **Configuration** > **Policies** > **VAS Settings** .
The VAS Settings dialog box appears.

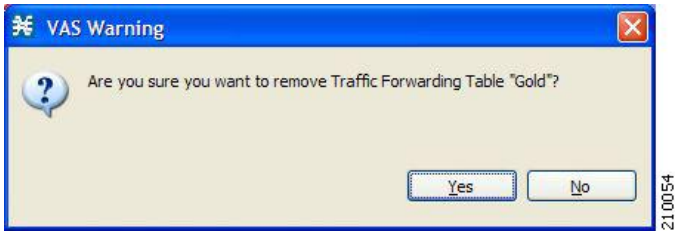
Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 Click the **Traffic Forwarding Tables** tab.

Step 4 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 5 Click the Delete (158940.jpg) icon.
A VAS Warning message appears.

Figure 306: VAS Warning



Step 6 Click **Yes**.
The selected table is deleted and is no longer displayed in the list of traffic-forwarding tables.

Step 7 Click **Close** .
The VAS Settings dialog box closes.

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.

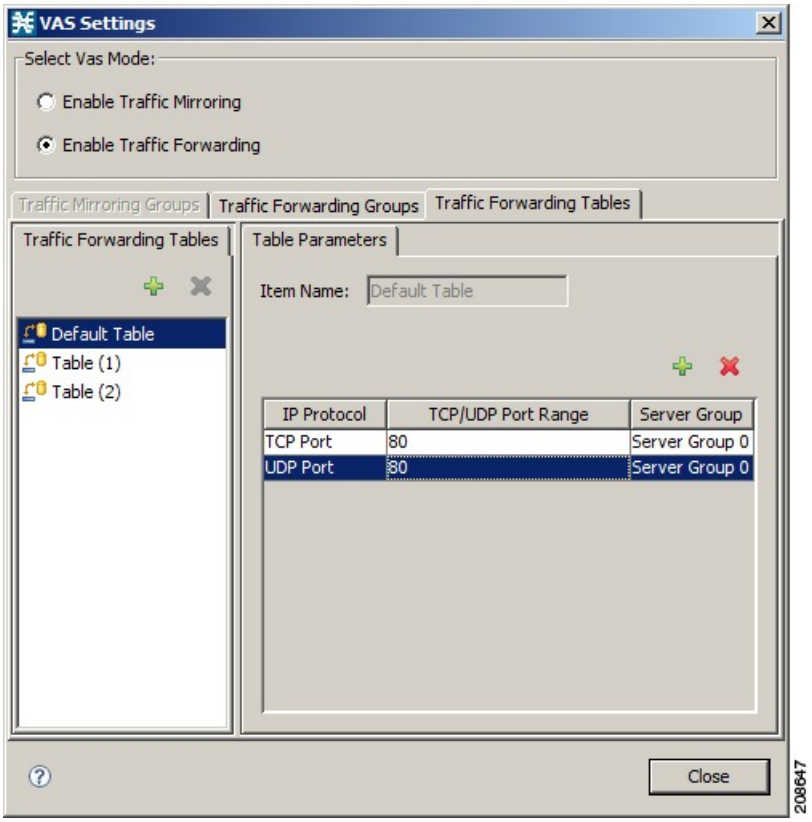
Procedure

Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies** > **VAS Settings**.
The VAS Settings dialog box appears.

Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 Click the **Traffic Forwarding Tables** tab.
The Traffic Forwarding Tables tab opens.

Figure 307: VAS Settings - Add VAS Traffic-Forwarding Tables



Step 4 In the Traffic Forwarding Tables area, click the Add (158725.jpg) icon.
A new table named Table (n), where n is a value from 1 through 63, is added to the list of traffic-forwarding tables in the Traffic Forwarding Tables area.
The table name is also displayed in the Item Name box in the Table Parameters tab.

Step 5 In the Item Name field, enter a unique and relevant name for the traffic-forwarding table.

You can now add table parameters to the new traffic-forwarding table, see “How to Add VAS Table Parameters” section.

Managing VAS Table Parameters Overview

A table parameter is an IP protocol type, an associated TCP/UDP port (where applicable), and a VAS server group or a range of IP addresses.

A traffic-forwarding table is a collection of related table parameters.

A traffic-forwarding table can contain up to 64 table parameters.

Adding VAS Table Parameters

You can add up to 64 table parameters to a traffic-forwarding table.

Procedure

Step 1 From the Policies tab in the left pane, choose Configuration > Policies > VAS Settings .
The VAS Settings dialog box appears.

Step 2 Click the Enable Traffic Forwarding radio button.

Step 3 Click the Traffic Forwarding Tables tab.
The Traffic Forwarding Tables tab opens.

Step 4 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 5 In the Traffic Parameters tab, click the Add (158725.jpg) icon.
A new table parameter is added to the list of table parameters in the Table Parameters tab.

Table 14: Table Parameter Default Values

Parameter	Default value
IP Protocol	
TCP Port	
TCP/UDP Port Range	
Parameter	Default value
IP Protocol	
TCP Port	
TCP/UDP Port Range	

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

Procedure

Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies** > **VAS Settings**.
The VAS Settings dialog box appears.

Step 2 Click the Enable Traffic Forwarding radio button.

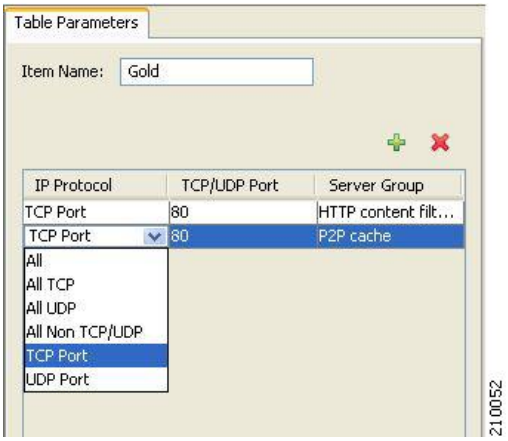
Step 3 Click the Traffic Forwarding Tables tab.
The Traffic Forwarding Tables tab opens.

Step 4 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 5 In the table in the Table Parameters tab select a protocol, port, and server group.

Step 6 Click in a cell in the IP Protocol column, and, from the drop-down list that opens, select an IP protocol type.

Figure 308: Table Parameters Tab

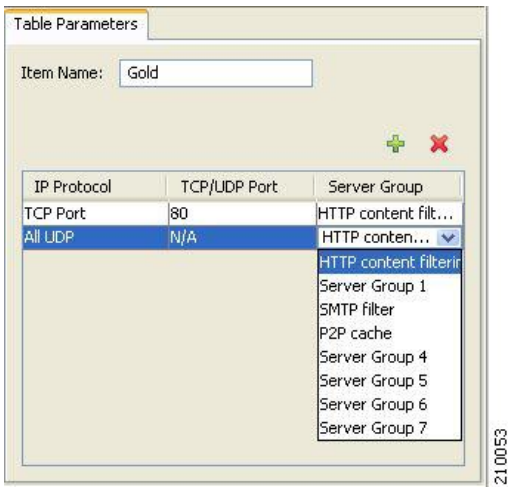


If you select All, All TCP, All UDP, or All Non TCP/UDP, “N/A” appears in the TCP/UDP Port cell when you move to another cell in the table.

Step 7 If you selected TCP Port or UDP Port, double-click in the cell in the TCP/UDP Port Range column, and enter the port number or a range of ports.

Step 8 Click in the cell in the Server Group column, and, from the drop-down list that opens, select a server group.

Figure 309: Tables Parameters Tab



Step 9 Click Close.
The VAS Settings dialog box closes.

Deleting VAS Table Parameters

Procedure

Step 1 From the Policies tab in the left pane, choose **Configuration** > **Policies** > **VAS Settings** .
The VAS Settings dialog box appears.

Step 2 Click the **Enable Traffic Forwarding** radio button.

Step 3 Click the **Traffic Forwarding Tables** tab.
The Traffic Forwarding Tables tab opens.

Step 4 From the list of traffic-forwarding tables in the Traffic Forwarding Tables area, select a table.

Step 5 From the list of table parameters in the Table Parameters tab, select a table parameter.

Step 6 Click the Delete ( ) icon.
The selected table parameter is deleted and is no longer displayed in the list of table parameters.

Step 7 Click Close .
The VAS Settings dialog box closes.

Managing the Protected URL Database

The Cisco SCE Protected URL Database is a database that contains a *blacklist*, a list of websites that are considered off limits or dangerous. You can configure the Cisco SCE to apply a specific action, such as blocking a site, when a subscriber attempts to access a site listed on the blacklist.

The database is encrypted so that no one, including the operator, can view the blacklist. The blacklist is managed on the Cisco SCE and cannot be withdrawn to the management PC.

RDRs are created when a subscriber attempts to access a link included in the blacklist. However, the RDRs do not contains the URL or Host information of the site.

To enable the blacklist feature:

Procedure

Step 1 Define an HTTP flavor.

Step 2 Create a blacklist service.

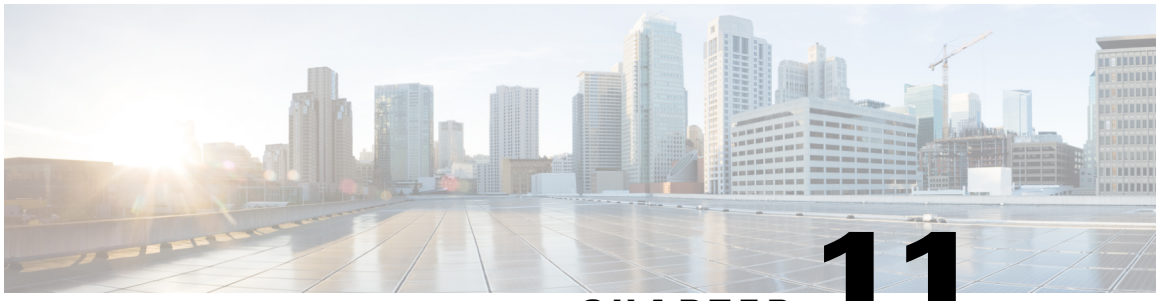
Step 3 Assign the HTTP flavor to the blacklist service.

Step 4 Create a rule for the blacklist service.

Step 5 Assign black list entries to the flavor, using the CLI.

What to Do Next

For more information about the Protected URL Database, see the Cisco Service Control URL Blacklisting Solution Guide .



CHAPTER 11

Subscriber Manager GUI Tool

This chapter describes how to use the Subscriber Manager (SM) graphical user interface (GUI) tool to configure subscribers in the Cisco Service Control SM database.

The SM GUI tool is especially useful when the Cisco Service Control SM holds a static list of subscribers. It is not applicable when Cisco SCA BB is operating in subscriberless mode (a mode in which control and analysis functions are available only at a global platform resolution) or in anonymous subscriber mode (a mode in which entities defined as IP addresses or VLANs are treated as subscribers). This chapter consists of these sections:

- Subscriber Manager GUI Tool Overview, page 457
- Connecting to a Cisco Service Control Subscriber Manager Overview, page 458
- Subscriber CSV Files Overview, page 461
- Subscriber Management Overview, page 462
- Monitoring SM Online Status, page 471

Subscriber Manager GUI Tool Overview

This chapter describes how to use the Subscriber Manager (SM) graphical user interface (GUI) tool to configure subscribers in the Cisco Service Control SM database.

The SM GUI tool is especially useful when the Cisco Service Control SM holds a static list of subscribers. It is not applicable when Cisco SCA BB is operating in subscriberless mode (a mode in which control and analysis functions are available only at a global platform resolution) or in anonymous subscriber mode (a mode in which entities defined as IP addresses or VLANs are treated as subscribers).

The SM GUI tool allows you to manage subscribers on a Cisco Service Control SM. The Cisco Service Control SM functions as middleware software that bridges between the OSS and the Cisco Service Control Engine (Cisco SCE) platforms. Cisco SCE platforms use the subscriber information to provide subscriber-aware functionality, per-subscriber reporting, and policy enforcement. Subscriber information is stored in the Cisco Service Control SM database and can be distributed between multiple platforms according to actual subscriber placement.

You can use the SM GUI tool to import and export subscriber files, and to perform operations on individual subscribers, such as:

- Add and delete a subscriber
- Edit parameters and show data of an existing subscriber
- Add and remove subscriber mappings
- Import subscribers from a CSV file
- Export subscribers to a CSV file
- Find subscriber or subscribers in a certain domain (filter)



Note To access a Cisco Service Control SM from the SM GUI tool, you must first add the Cisco Service Control SM to the Site Manager tree in the Network Navigator tool (see "How to Add Subscriber Manager Devices to a Site" section).

The SM GUI tool provides only a subset of the functionality that the SM Command-Line Utility provides. For more information about the Cisco Service Control SM, see the Cisco Service Control Management Suite Subscriber Manager User Guide.

Connecting to a Cisco Service Control Subscriber Manager Overview

You can connect to a Cisco Service Control Subscriber Manager:

- From the Network Navigator tool
- From anywhere else in the Console
- From the Subscriber Manager GUI tool



Note The SM GUI tool performs authentication on the Cisco Service Control Subscriber Manager by opening a PRPC connection to port 14374 and attempting to log in using the username and password that you entered in the Password Management dialog box. If a PRPC server with this user is not running on the Cisco Service Control Subscriber Manager, authentication fails. If you have changed the PRPC port on the Cisco Service Control Subscriber Manager, see "User Authentication" section.

Connecting to a Cisco Service Control Subscriber Manager from the Network Navigator

Procedure

Step 1 In the Site Manager tree in the Network Navigator tab, right-click an SM device.

A popup menu appears.

Figure 310: SM Device Popup Menu



Step 2 From the menu, select **Manage Subscribers**.
A Password Management dialog box appears.

Step 3 Enter the appropriate password.
For more information, see the "Password Management" section.

Step 4 Click **Connecting**.
The Password Management dialog box closes. A Connecting to progress bar appears.

The system connects to the Cisco Service Control Subscriber Manager.

Connecting to a Cisco Service Control Subscriber Manager from the Console

Note If you are already in the Subscriber Manager GUI tool, start at Step 3.

Procedure

Step 1 From the Console main menu, choose**Tools** > **Subscriber Manager**.
The Subscriber Manager GUI tool opens. A Subscriber Manager is not connected message appears.

Figure 311: Subscriber Manager is not Connected

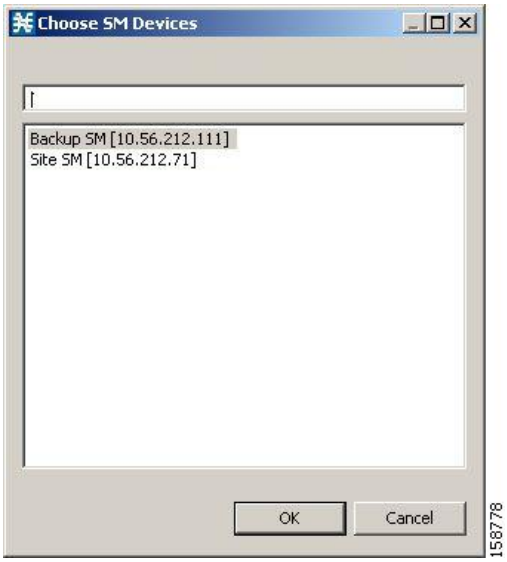


Step 2 Click OK.

The Subscriber Manager is not connected message closes.

Step 3 In the Subscriber Manager GUI toolbar, click the Connect to an SM ( ) icon.
If more than one Cisco Service Control SM device is configured in the Network Navigator, the Choose SM Devices dialog box appears.

Figure 312: Choose SM Devices



Step 4 Select a device and click OK.
A Password Management dialog box appears.

Step 5 Enter the appropriate password.
For more information, see “Password Management” section

Step 6 Click **Connecting**.
The Password Management dialog box closes. A Connecting to progress bar appears.

The system connects to the Cisco Service Control SM. The Import subscribers from CSV file ( ), the Export subscribers to CSV file , and the Disconnect from SM icons are enabled.

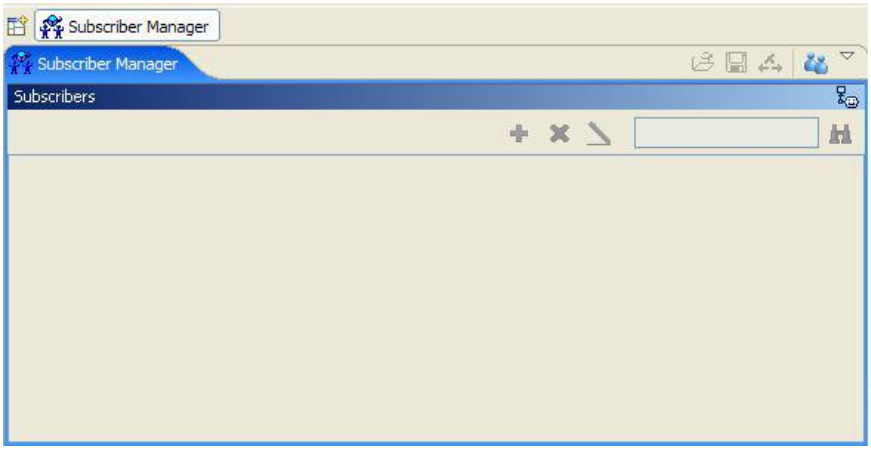
Disconnecting from the Current Cisco Service Control Subscriber Manager

Procedure

In the SM GUI toolbar, click the Disconnect from SM ( ) icon.

The Console disconnects from the Cisco Service Control Subscriber Manager, but the SM GUI tool remains open. The Import subscribers from CSV file ( ) , the Export subscribers to CSV file ( ) , and the Disconnect from SM ( ) icons are dimmed. The subscriber list is empty.

Figure 313: Subscriber Manager List



Subscriber CSV Files Overview

Because of the large number of subscribers that must be introduced into the system, it is not feasible to enter subscriber information manually. Usually a RADIUS server (or some similar source) generates the subscriber information. This information is then imported into the Subscriber Manager GUI tool.

You can also export updated subscriber information to a CSV file.

The format of subscriber CSV files is described in the “CSV File Formats” chapter of Cisco Service Control Application for Broadband Reference Guide.

Importing Subscriber Information from a CSV File

You can import subscriber data that was exported to a CSV file into the Subscriber Manager GUI tool.

Before You Begin

Confirm that the subaware.pro file in the Cisco Service Control Subscriber Manager is configured to import the required type of subscribers—IPv4 subscribers or IPv4 and IPv6 subscribers. If required, make necessary changes to subaware.pro file. For more details on configuring the subaware.pro file, see the Cisco Service Control Management Suite Subscriber Manager User Guide.

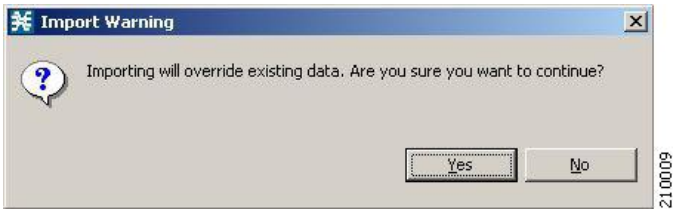
Procedure

Step 1 In the SM GUI toolbar, click the Import subscribers from CSV file ( ) icon.

An Import from File dialog box appears.

Step 2 Browse to the file that is to be imported and click Open.
An Import Warning message appears.

Figure 314: Import Warning



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 Information to a CSV File

You can export subscriber information to a CSV file (for example, when data in the Cisco Service Control SM database is updated).

Procedure

Step 1 Select the subscribers whose data you want to save.
See the "Selecting Subscribers" section.

Step 2 In the SM toolbar, click the Export subscribers to CSV file  icon.
An Export to File dialog box appears.

Step 3 Browse to the folder in which you want to save the exported file.

Step 4 In the File name field, enter a file name.

Step 5 Click Save.
The Export to File dialog box closes.

The selected subscribers are saved to the CSV file.

Subscriber Management Overview

After importing subscribers into the system, you can maintain and update the database.

You can perform the following operations:

Subscriber Information

In the SM GUI, you can see a list of all the subscribers currently introduced into Cisco SCA BB. Use this list to manage individual subscribers or groups of subscribers. Use the Find function to display a subset of the subscribers (see Finding a Subscriber or Group of Subscribers).

The SM GUI is composed of a console view at the bottom and a device view at the top. The console shows the log messages. The device view has the following columns:

- Subscriber ID—Name of the subscriber in the system.
- Domain—Domain to which the subscriber is assigned. The names of the Cisco SCE platforms that belong to each domain appear in square brackets.
- Network Mappings—IP address, range of IP addresses, or VLAN tag mapped to the subscriber.
- Properties—Various properties assigned to the subscriber (Package ID, Monitor State, Up Vlink ID, Down Vlink ID).
- Custom Properties—Displayed as key value pairs.

Figure 315: Subscriber Manager GUI - Subscriber List

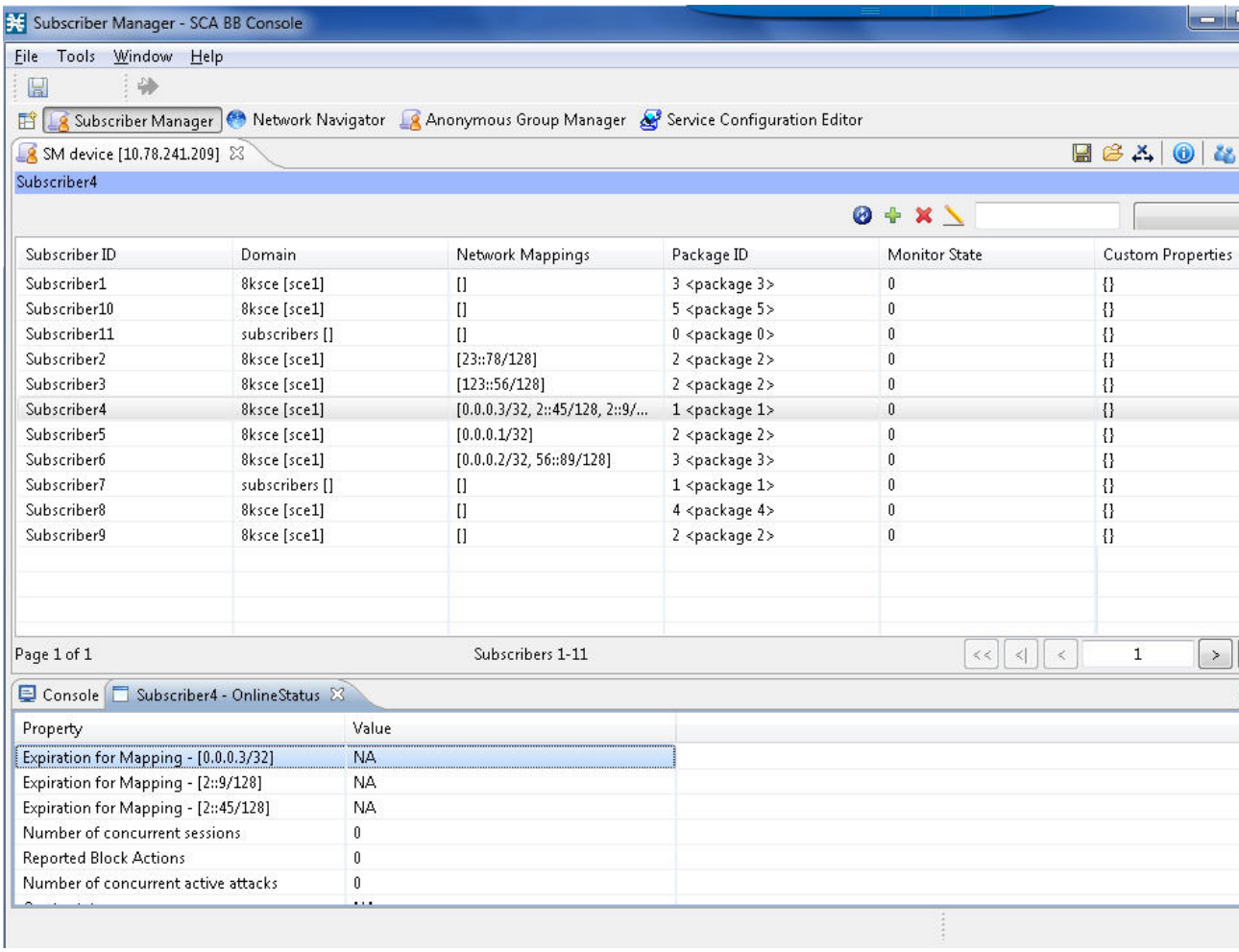
Table 15: SM GUI Icon Descriptions

Icon	Description
	Delete all subscribers (if enabled).
	Export subscribers to CSV file.
	Import subscribers from CSV file.
	Disconnect from SM.
	View online status (opens SM online status window).
	Connect to an SM.
	Refresh the list of subscribers.
	Add subscriber.
	Remove subscriber.
	Edit subscriber.

By right-clicking on a specific subscriber, you can perform various actions, including:

- Edit subscriber data.
- Delete the subscriber.
- Display the online status of the subscriber, including:
  - Expiration or aging time (if any)
  - Number of concurrent sessions
  - Reported block actions
  - Number of concurrent active attacks
  - Quota status (if any)
  - Subscriber OS information
- View information on multiple subscriber in multiple windows.

Figure 316: Subscriber Manager GUI - Subscriber Online Status



From the menu bar, you can select and open the Preferences page. When the Subscriber Manager is selected in the left pane, you can do the following:

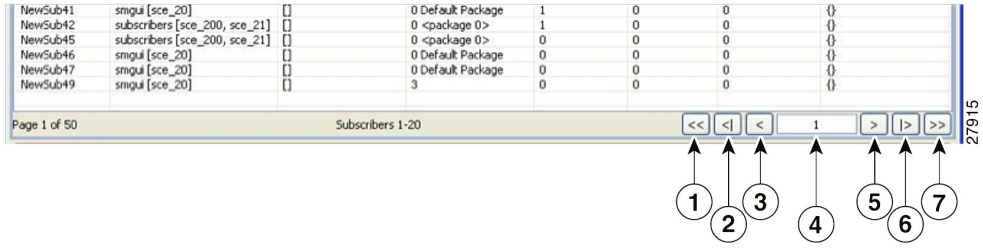
- Specify the number of subscriber records to be listed in the main display table.
- Enable or disable the “Remove All Subscribers” functionality.
- Enable or disable the enhanced subscriber data mode; if enabled, the Up Vlink ID and Down Vlink ID columns are displayed in the table.

Overview of How to Find and Select Subscribers

The SM GUI tool retrieves subscribers in bulks of 1000 subscribers.

If the number of subscribers are more than that can be displayed in a standard view, then the information is presented in multiple pages. You can navigate to the remaining groups of subscribers using the various pagination buttons.

Figure 317: Subscriber Manager GUI - Pagination Buttons



- 1. Get previous bulk.
- 2. Get first page.
- 3. Get previous page.
- 4. Enter page number.
- 5. Get next page.
- 6. Get last page.
- 7. Get next bulk.

For ease of use, the SM GUI tool incorporates two standard features:

- Find—Search for a specific subscriber.
- Multiple Select—Select a range of subscribers or a number of individual subscribers.

Finding a Subscriber or Group of Subscribers

Use the Find feature to find a specific subscriber or a group of subscribers according to a subscriber ID prefix. This feature is useful for editing the parameters of either a specific subscriber or a group of subscribers (see “Editing Subscriber Details” section.

Procedure

Step 1 In the Find field enter the prefix to be matched.

Figure 318: Find Field



Step 2 Click the Find Subscribers ( ) icon.
You see a list of only the subscribers that match the specified prefix.

The search criteria is selected in the drop-down list next to the Find field. Search by:

- Prefix
- Domain name
- Package ID

Selecting Subscribers

You can edit, export, or delete a group of subscribers at one time by selecting subscribers displayed in the subscriber list. The group may be either of the following:

Selecting a Range of Subscribers

Procedure

Step 1 Select the first subscriber in the range.

Step 2 Press the Shift key while clicking the last subscriber in the range.
You can combine this function with the search function; search for specific subscribers and then select the entire range.
All subscribers within the range are selected.

Selecting a Number of Noncontiguous Subscribers

Procedure

Press the Ctrl key while selecting multiple subscribers.

You can combine this function with selecting a range of subscribers; first, select the range of subscribers, and then select additional subscribers.

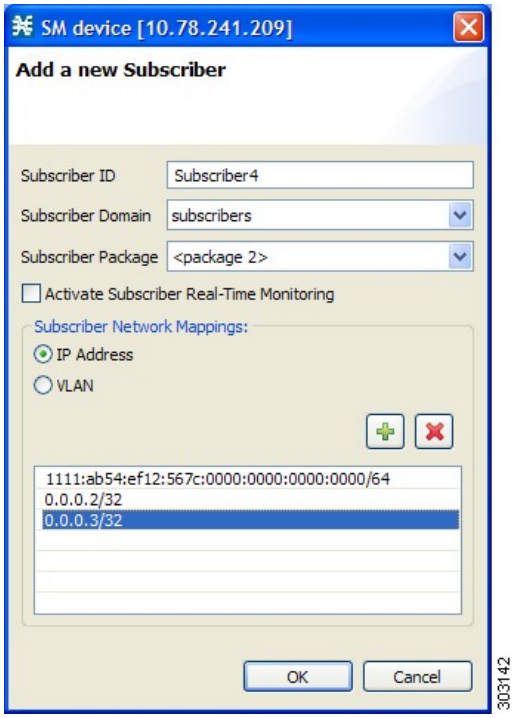
Adding a Subscriber

You can add additional individual subscribers to the Cisco Service Control Subscriber Manager. To add large number of subscribers, export their information from a RADIUS (or DHCP) server to a CSV file, and then import the CSV file. For details on importing the CSV files, see “Working with Subscriber CSV Files” section.

Procedure

Step 1 In the SM GUI toolbar, click the Add Subscriber ( ) icon.
The Add a New Subscriber dialog box appears.

Figure 319: Add a New Subscriber



Step 2 In the Subscriber ID field, enter text that identifies the subscriber.

Step 3 From the Subscriber Domain drop-down list, select the appropriate domain for the new subscriber.

Step 4 From the Subscriber Package drop-down list, select a package to assign to this subscriber.
The contents of the list depend on the selected subscriber domain.

Step 5 To activate subscriber real-time monitoring, check the Activate Subscriber Real-time Monitoring check box.

This sets the “monitor” property to 1 and causes the Cisco SCE application to generate Real-Time Subscriber Usage RDRs for this subscriber.

Step 6 Define subscriber network mappings. If you are not going to define network mappings for this subscriber, continue at Step 10.
The system supports either IP addresses or VLAN tags as network identification for subscribers. The Cisco Service Control solution supports an IP prefix range of 0 to 32 for IPv4 addresses and 32 to 34 for IPv6 addresses. Select one of the Subscriber Network Mappings radio buttons:

- IP Address
- VLAN

Note We recommend that you do not assign the same IPv6 address to different subscribers with different prefix values.

Step 7 Click **Add** ( ) icon to add a network mapping of the type selected.
A new network-mapping entry is added to the subscriber network mappings list, displaying a default value

Step 8 Edit the network-mapping entry.

Step 9 Repeat Steps 7 and 8 for other network mappings.

Step 10 Click OK .
The Add a New Subscriber dialog box closes.

The new subscriber is added to the database and joins the subscriber list displayed in the SM GUI tool.

Editing Subscriber Details

You can edit parameters for each subscriber.

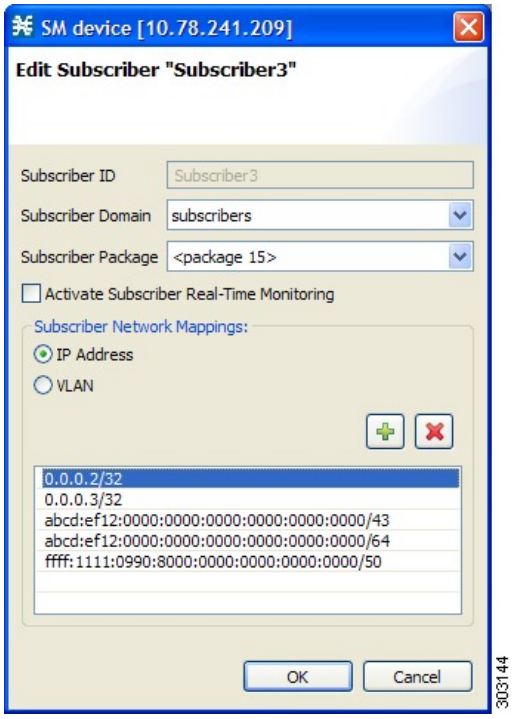
Procedure

Step 1 Find and select a subscriber. (See the “How to Find a Subscriber or Group of Subscribers” section.)

Step 2 In the SM toolbar, click the Edit Subscriber ( ) icon.

The Edit Subscriber dialog box appears.

Figure 320: Edit Subscriber



Step 3 Modify subscriber details.

a) Edit the entry in the Subscriber ID field.

b) From the Subscriber Domain drop-down list, select a subscriber domain.

c) 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.

d) Check or uncheck the **Activate Subscriber Real-time Monitoring** check box. If you are not editing the network mappings for this subscriber, continue at Step 5.

Step 4 Modify subscriber network mappings. The Cisco Service Control solution supports an IP prefix range of 0 to 32 for IPv4 addresses and 32 to 34 for IPv6 addresses. To modify the Subscriber Network Mappings:

Step 5 Click one of the Subscriber Network Mappings radio buttons:

- IP Address
- VLAN

Step 6 To add a new network mapping to the list, click the Add ( ) icon, and edit the network-mapping field that is added to the Subscriber Network Mappings list.

Step 7 To delete a network mapping from the list, select an entry in the subscriber network mappings list and click the Delete ( ) icon.

Step 8 Click Apply.

The Edit Subscriber dialog box closes.

The modified subscriber information is saved to the database and displayed in the subscriber list in the SM GUI tool.

Deleting a Subscriber from the Database

You can delete subscribers from the database.

Procedure

Step 1 Select a single subscriber or a group of subscribers.
See the "Selecting Subscribers" section.

Step 2 In the SM toolbar, click the Delete Subscriber ( ) icon.
The system asks for confirmation before deleting the selected subscribers.

Figure 321: Subscriber Warning



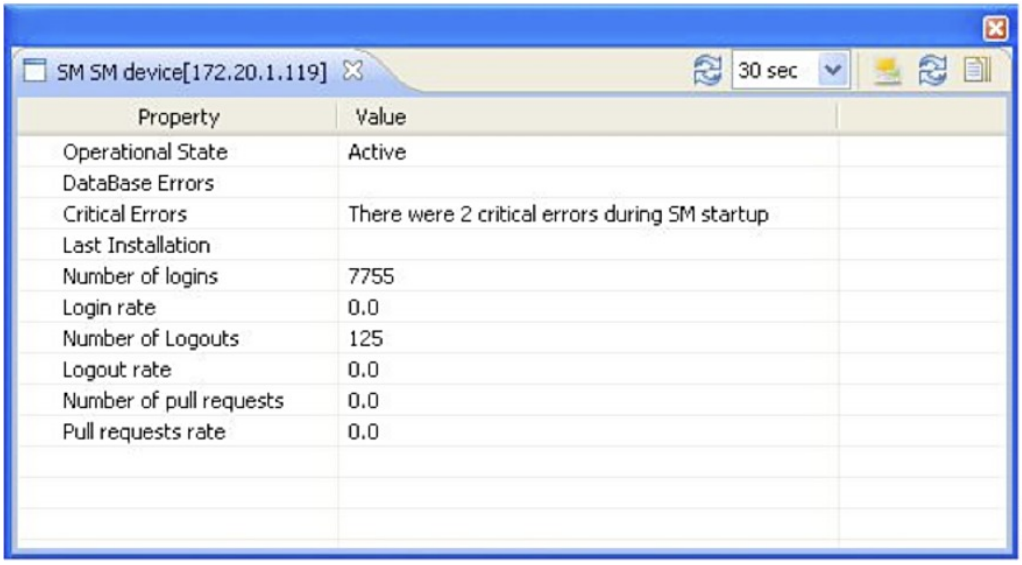
Step 3 Click Yes to confirm.

The selected subscribers are deleted from the database and removed from the subscriber list displayed in the SM GUI tool.

Monitoring SM Online Status

The SM online status window provides real-time status of the SM operation by displaying the main properties of the SM.

Figure 322: SM Online Status Window



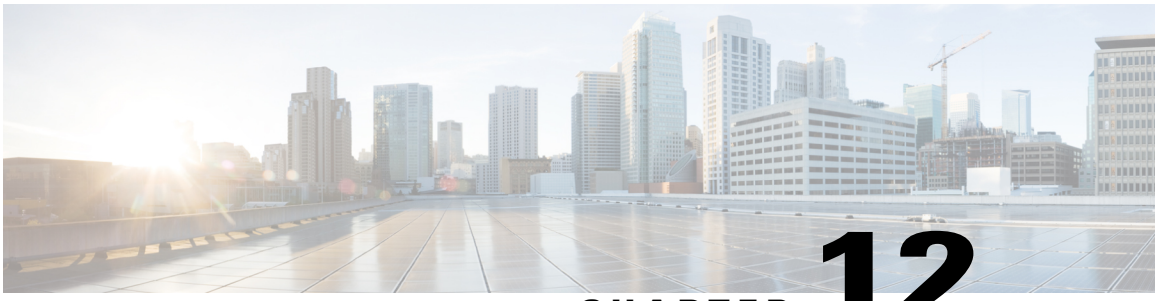
Procedure

To open the SM Online Status window, click on the Open ( ) icon in the main GUI toolbar. The icons are grouped in the toolbar at the upper right corner of the SM Online Status window.

Table 16: SM Online Status Window Icon Descriptions

Icon	Description
	Autorefresh , the drop-down list shows selectable time interval options (default 30 seconds)
	Copy all properties and values to the clipboard (or right-click a single property to copy)

Icon	Description
	Always on top (enable or disable place status window on top of other windows)



CHAPTER 12

Anonymous Group Manager GUI Tool

This chapter provides details on the Anonymous Group Manager GUI tool and how to manager Anonymous Groups using the Cisco SCA BB. This chapter describes how to use the Anonymous Group Manager graphical user interface (GUI) tool to configure anonymous groups in a Cisco SCE. This chapter consists of these sections:

- Using the Anonymous Group Manager GUI Tool, page 473
- Introduction to Managing Anonymous Groups, page 474
- Working with Anonymous Groups CSV Files , page 484

Using the Anonymous Group Manager GUI Tool

You can use the Anonymous Group Manager GUI tool to import and export subscriber files, and to perform these operations on anonymous groups:

- Add and delete an anonymous group
- View the subscribers in a specific anonymous group
- Delete all anonymous groups
- View the configuration of a specific anonymous group
- Filter subscribers
- View online status of the subscriber
- View OS information of the subscribers in anonymous group
- Edit subscriber properties
- Import anonymous groups from a CSV file
- Export anonymous groups to a CSV file
- Export subscribers of a certain group to CSV file

Software-based support for IPv6 subscribers is available on .

For details on Anonymous Groups, Subscriber templates, and CSV file formats, see the .

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

Introduction to Managing Anonymous Groups

After importing subscribers into the system, you can maintain and update the database.

You can perform these tasks:

- Add and delete an anonymous group
- View the subscribers in a specific anonymous group
- View the configuration of a specific anonymous group
- Delete all anonymous groups in the Cisco SCE
- Filter subscribers
- View online status of the subscriber
- Edit subscriber properties

This section contains information on:

Anonymous Group Manager Information

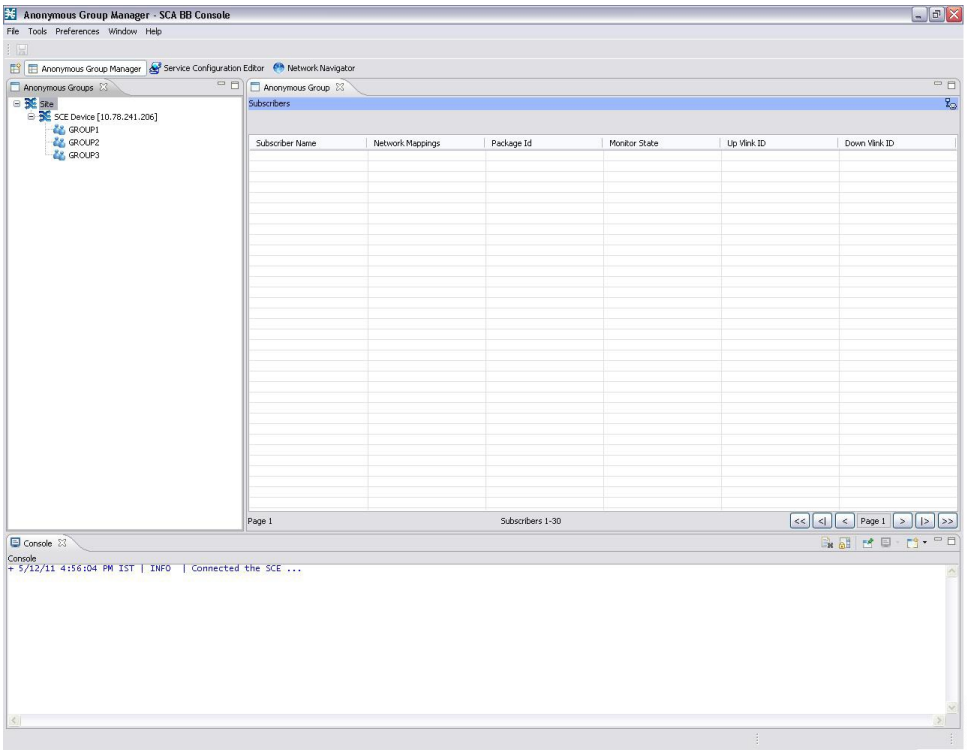
In the Anonymous Group Manager GUI, you can see a list of anonymous groups configured in a Cisco SCE. Use this list to manage individual anonymous group or multiple groups of subscriber tables stacked together, and the subscribers in each anonymous group.

The Anonymous Group Manager GUI is composed of a console view at the bottom and a device view at the top. The console shows the log messages. The anonymous group view within the group folder has the following columns in a subscriber table:

- Subscriber Name—Name of the subscriber in the system.
- Mappings—IP address, range of IP addresses, or VLAN tag mapped to the subscriber.
- Package ID
- Monitor State
- Up VLINK ID
- Down VLINK ID

• Owner—Owner of the subscriber (For example, Subscriber Manager Device)

Figure 323: Anonymous Group Manager GUI - Group List



Right-click on the specific subscriber to perform various actions including the following:

• Edit subscriber data.

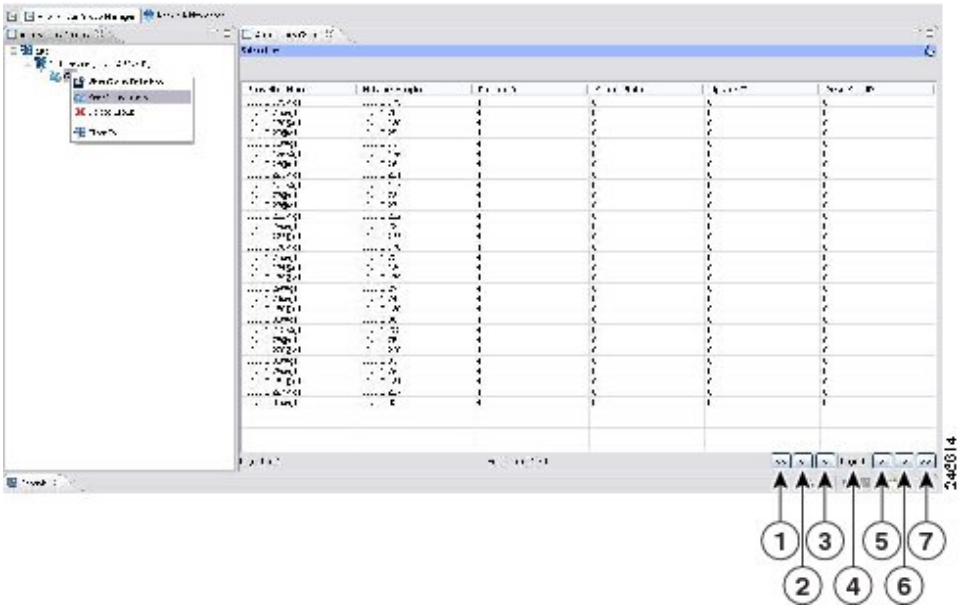
• View the online status of the subscriber

Finding and Selecting Subscribers Overview

The Anonymous Group Manager GUI tool retrieves subscribers in bulks of 1000 subscribers. Subscriber information is displayed in a standard view. If there are more subscribers than that can be displayed in the

standard view, then the information is displayed in pages. You can use the various pagination buttons to navigate between the pages.

Figure 324: Anonymous Group Manager GUI - Pagination Buttons



1. Get previous bulk.
2. Get first page.
3. Get previous page.
4. Enter page number.
5. Get next page.
6. Get last page.
7. Get next bulk.

For ease of use, the Anonymous Group Manager GUI tool incorporates two standard features:

- Filter—You can filter the subscriber list based on the packageID, downVlinkId, monitor, and upVlinkId.

- Multiple Select—Select a range of subscribers or a number of individual subscribers.

Figure 325: Filter Anonymous Subscriber



Selecting Subscribers Overview

You can edit, export, or delete a group of subscribers at one time by selecting subscribers displayed in the subscriber list. The group may be either of the following:

- A range of contiguous subscribers
- A number of noncontiguous subscribers

Selecting a Range of Subscribers

Procedure

Step 1 Select the first subscriber in the range.

Step 2 Press the Shift key while clicking the last subscriber in the range.

All subscribers within the range are selected. You can combine this function with the search function; search for specific subscribers and then select the entire range.

Selecting a Number of Noncontiguous Subscribers

Procedure

Press the Ctrl key while selecting multiple subscribers.
You can combine this function with selecting a range of subscribers; first, select the range of subscribers, and then select additional subscribers.

Adding a Cisco SCE to the Anonymous Group Manager GUI Tool

All SCEs added to Cisco SCA BB Network Navigator appears in the site list of the Anonymous Group Manager GUI Tool.
For details on adding SCEs through Network Navigator, see the Adding Cisco SCE Devices to a Site section.

Adding a New Anonymous Group in a Cisco SCE Device

Procedure

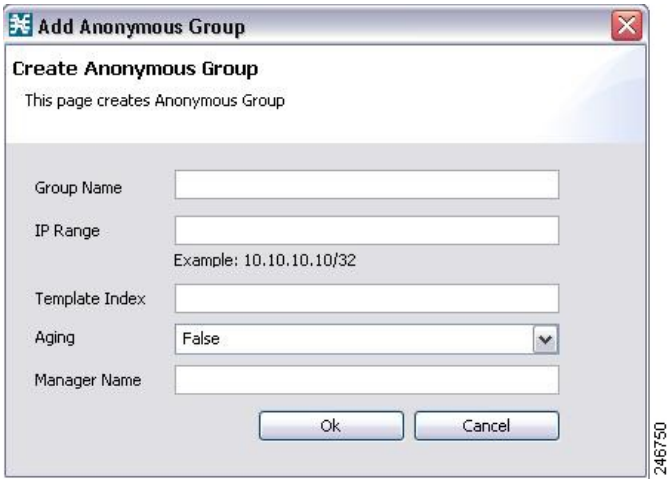
Step 1 From the Console main menu, choose Tools > Anonymous Group Manager.
The Anonymous Group Manager tool opens.

Step 2 If the device is not listed in the Site list, add the device using the Network Navigator.

Step 3 Right-click the corresponding Cisco SCE device, and select Add a New Group.
A Password Management window appears with the Device, Device Type, and Service information.

Step 4 Enter the User Name and Password. For details on password management, see the Password Management section.
The Add Anonymous Group page appears.

Figure 326: Add Anonymous Group



Step 5 Enter the Group Name, IP Range, Template Index, and Manager Name.

Step 6 Select the Aging option from the drop-down list.

Step 7 Click **Ok**.
The new anonymous group is added to the specific Cisco SCE.

Adding a New IPv6 Anonymous Group in a Cisco SCE Device

Procedure

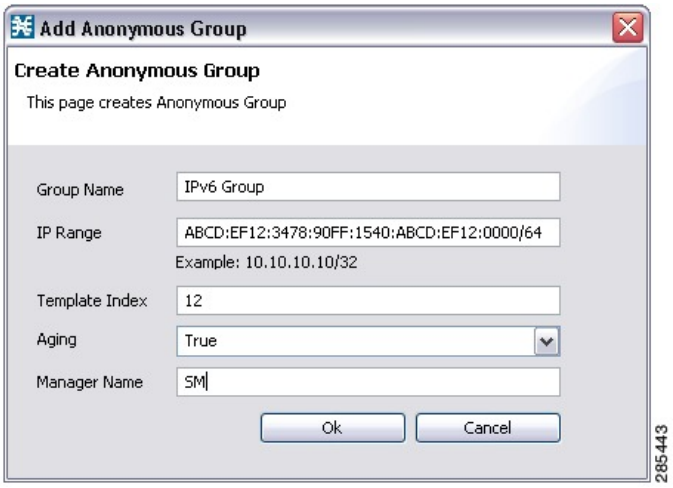
Step 1 From the Console main menu, choose Tools > Anonymous Group Manager .
The Anonymous Group Manager tool opens.

Step 2 If the device is not listed in the Site list, add the device using the Network Navigator.

Step 3 Right-click on the Cisco SCE, and select Add a New Group .
A Password Management window appears with the Device, Device Type, and Service information.

Step 4 Enter the User Name and Password. For details on password management, see the Password Management section.
The Add Anonymous Group page appears.

Figure 327: Add IPv6 Anonymous Group



Step 5 Enter the following details:

- Group Name
- IPv6 Range with a prefix value of 0 to 64
- Template Index
- Manager Name

Step 6 Select the Aging option from the drop-down list.

Step 7 Click Ok .
The new anonymous group is added to the specific Cisco SCE device.

Viewing the Configuration of a Specific Anonymous Group

Procedure

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

Figure 328: Anonymous Group Manager Tool

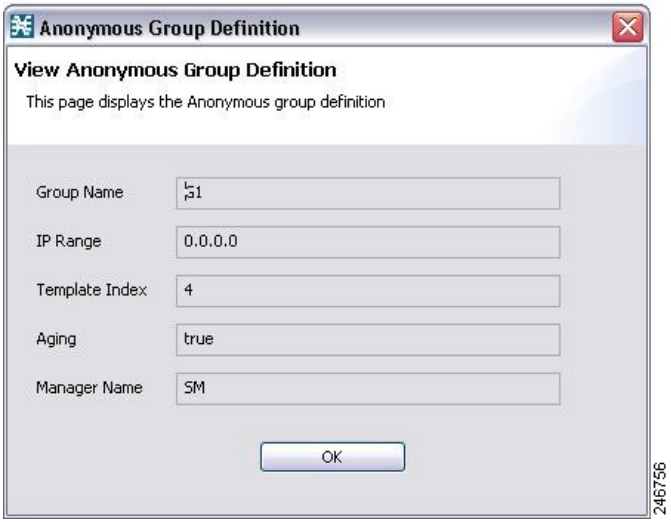
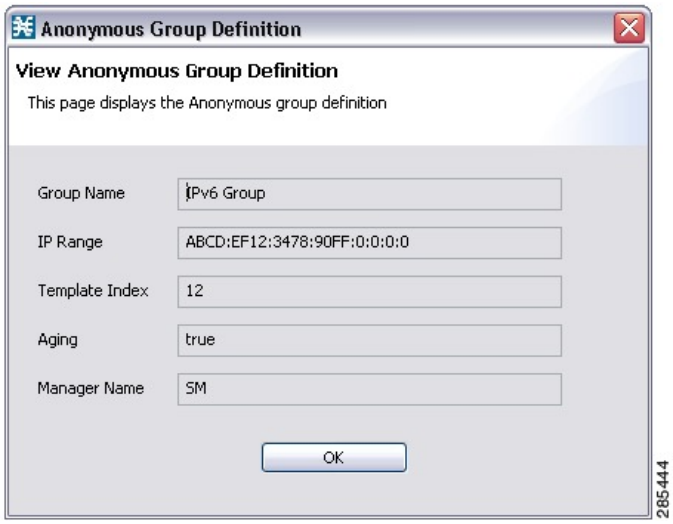


Figure 329: IPv6 Anonymous Group Manager Tool



Step 2 In the Site list, right-click the corresponding Anonymous Group, and select View Group Definition.

Deleting An Anonymous Groups in a Cisco SCE

Procedure

Step 1 From the Console main menu, choose Tools > Anonymous Group Manager .
The Anonymous Group Manager tool opens.

Step 2 From the Site list, click on the Cisco SCE from which you plan to delete the Anonymous Group.
The Anonymous Groups in the Cisco SCE appears.

Step 3 Right-click on the Anonymous group to delete, and select Delete.
A confirmation dialog box appears.

Figure 330: Confirmation Dialog Box



Step 4 Click Yes.

Deleting All Anonymous Groups in a Cisco SCE

Procedure

Step 1 From the Console main menu, choose Tools > Anonymous Group Manager .
The Anonymous Group Manager tool opens.

Step 2 From the Site list, right-click on the Cisco SCE from which you plan to delete the Anonymous Groups and select Delete Groups.

A confirmation dialog box appears.

Figure 331: Confirmation Dialog Box



Step 3 Click Yes.

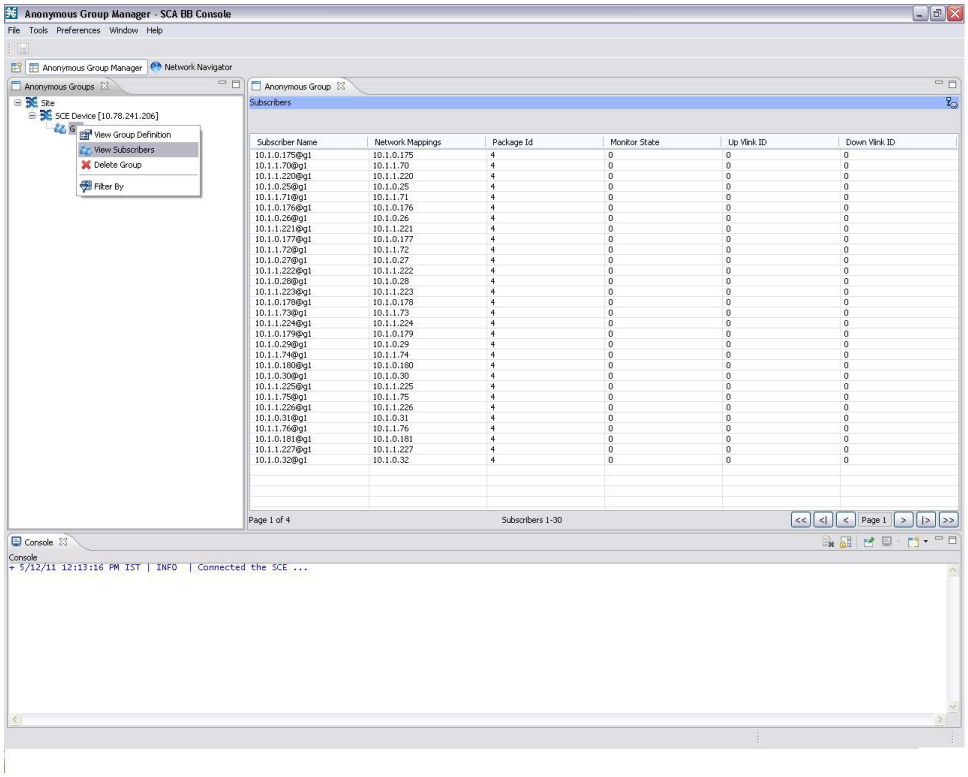
Viewing Subscribers in a Specific Anonymous Group

Procedure

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

The Anonymous Group Manager tool opens.

Figure 332: Anonymous Group Manager Tool



Step 2 In the Site list, right-click the Anonymous Group, and select View Subscribers.
The list of subscribers appears in the Anonymous Group tab near the Console tab.

Viewing the Online Status of a Subscriber

Procedure

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

Step 2 In the Site list, right-click the Anonymous Group, and select **View Subscribers**.
The list of subscribers appears in the Anonymous Group pane.

Step 3 Right-click in the subscriber row, and select **View Online Status**.
The online status appears.

Editing the Subscriber Properties

Procedure

Step 1 From the Console main menu, choose Tools > Anonymous Group Manager .
The Anonymous Group Manager tool opens.

Step 2 In the Site list, right-click the Anonymous Group, and select View Subscribers.
The list of subscribers appears in the Anonymous Group pane.

Step 3 Right-click in the subscriber row, and select Edit Subscriber .
The Edit Subscriber dialog box appears.

Step 4 Modify the required fields from the following:

- Package ID
- Monitor State
- UpVlinkId
- DownVlinkId

Step 5 Click OK .

Removing Subscribers from an Anonymous Group in a Cisco SCE

Procedure

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

Step 2 In the Site list, click the **Anonymous Group**, and select **View Subscribers**.
The list of subscribers appears in the Anonymous Group pane.

Step 3 Right-click in the subscriber row, and select **Remove the Subscriber**.
A confirmation dialog box appears.

Step 4 Click OK .

Working with Anonymous Groups CSV Files

With Anonymous Group GUI tool, you can:

- Import anonymous groups from a CSV file
- Export anonymous groups to a CSV file

- Export subscribers of a certain anonymous group to CSV file

The format of subscriber CSV files is described in the “CSV File Formats” chapter of Cisco Service Control Application for Broadband Reference Guide.

This section explains the following procedures:

- Importing Anonymous Groups from a CSV File
- Exporting Anonymous Groups to a CSV File

You can import subscriber data that was exported to a CSV file using the Anonymous Group Manager GUI tool. This feature supports only one Cisco SCE at a time.

Importing Anonymous Groups from a CSV File

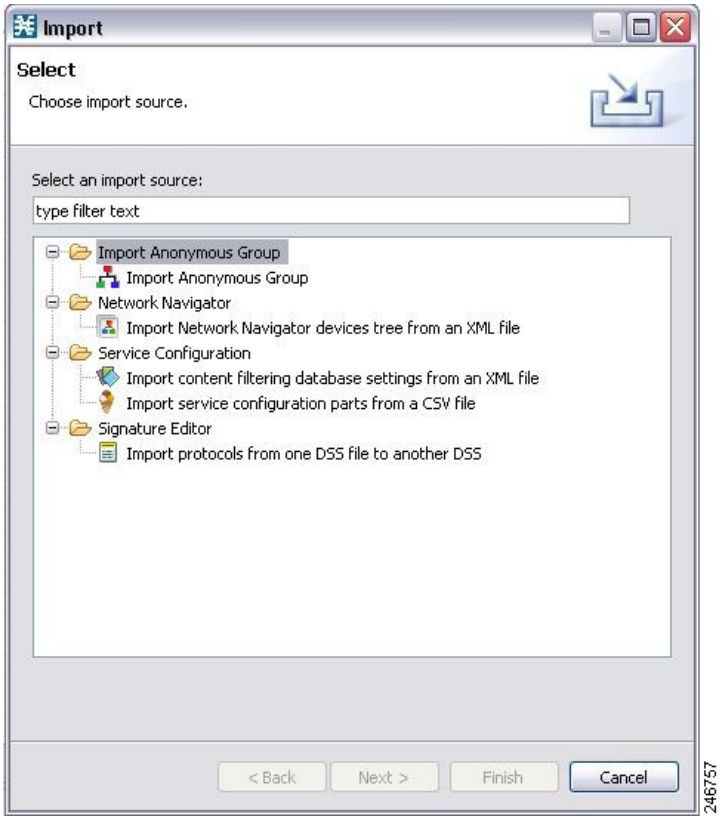
Procedure

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

Step 2 In the Site list in **Anonymous Group Manager** tool, click the Cisco SCE for which you want to import the Anonymous Groups.

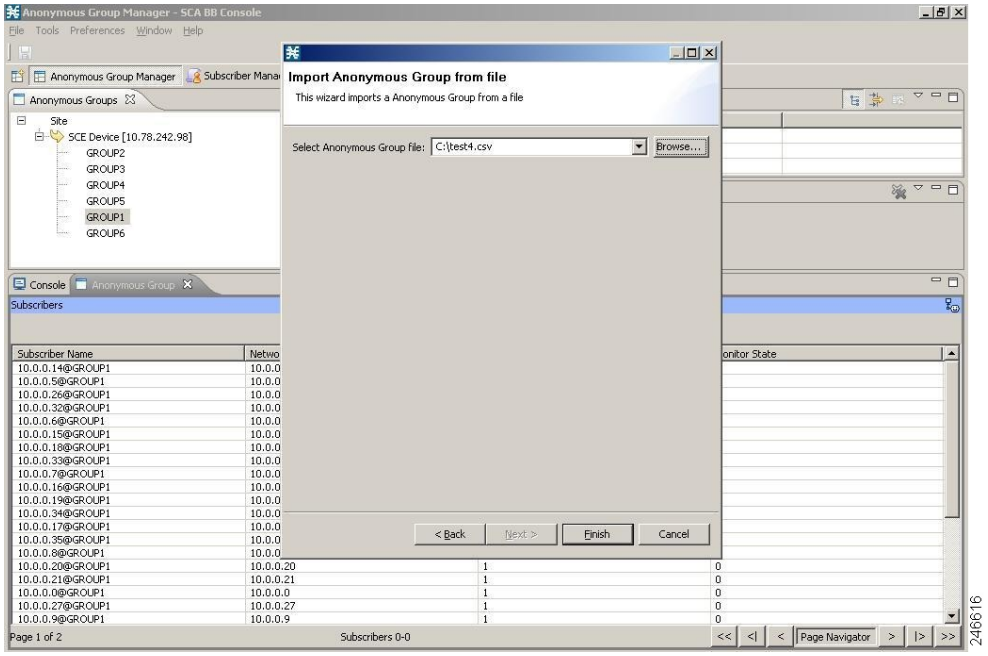
Step 3 Select **File** > **Import** .

Figure 333: Import Dialog Box



Step 4 Click **Next**.

Figure 334: Import Anonymous Groups from File Dialog Box



Step 5 In the **Import Anonymous Groups from File** dialog box, browse to the file that is to be imported and click **Finish** .
The selected file is imported into the Anonymous Group Manager GUI tool; the imported subscribers are listed in the subscriber list.

Exporting Anonymous Groups to a CSV File

You can export anonymous group information to a CSV file.

Procedure

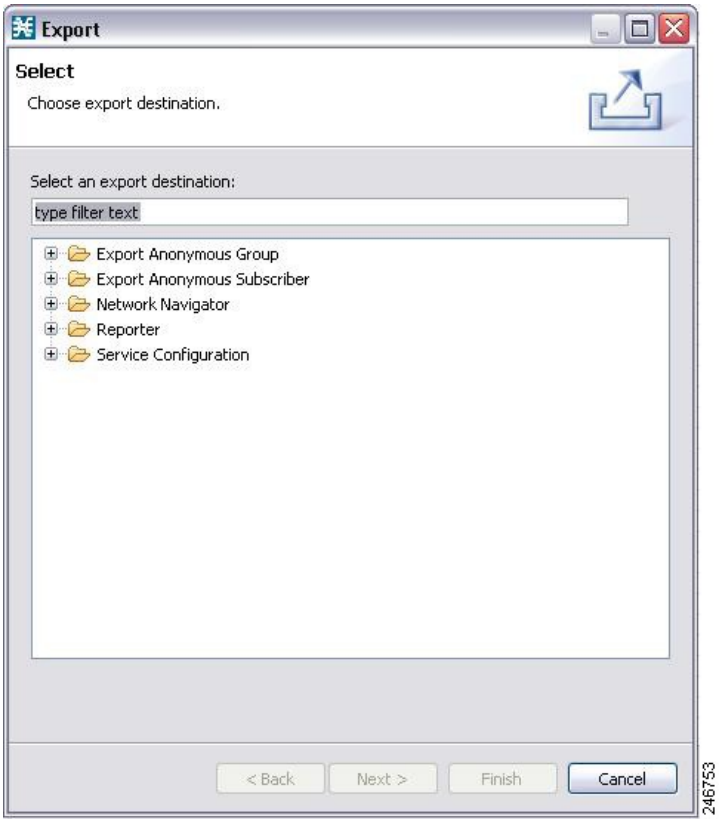
Step 1 From the Console main menu, choose Tools > Anonymous Group Manager .
The Anonymous Group Manager tool opens.

Step 2 In the Site list, click the Cisco SCE for which you want to export the Anonymous Groups.

Step 3 Select File > Export .

The Export dialog box appears.

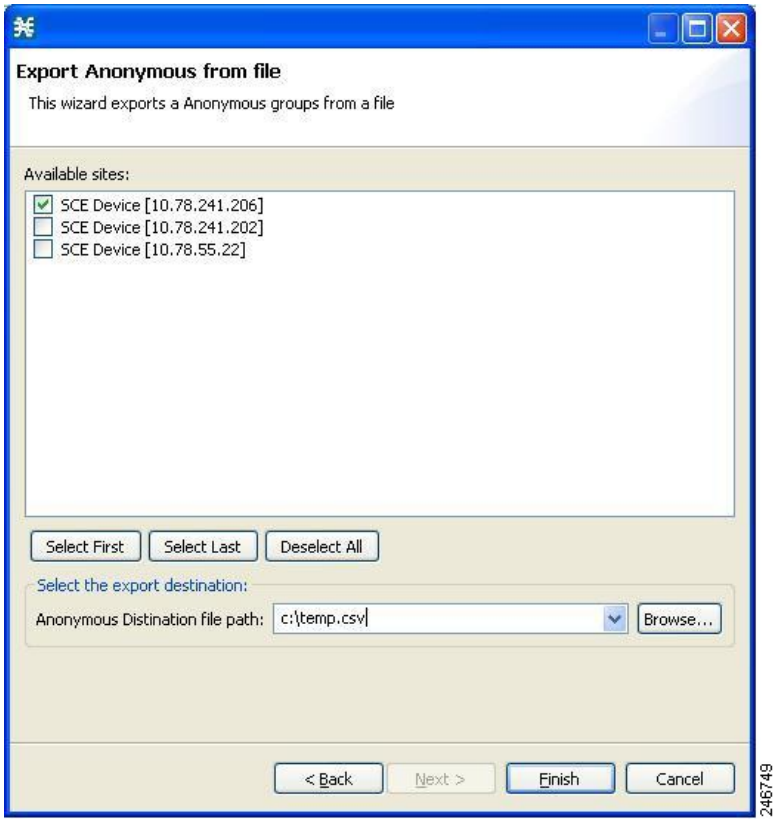
Figure 335: Export Dialog Box



Step 4 Click Next.

The Export Anonymous Groups from File dialog box appears.

Figure 336: Export Anonymous Groups from File Dialog Box



Step 5 Select the Cisco SCE Device and the Anonymous Groups to be exported.

Step 6 Select the Export destination and click Finish .
The Export from File dialog box closes. The Anonymous Group Information is exported to the CSV file.

Exporting Information on Subscribers of an Anonymous Group to CSV File

To export information of all subscribers of an anonymous group to a CSV file, complete these steps:

Procedure

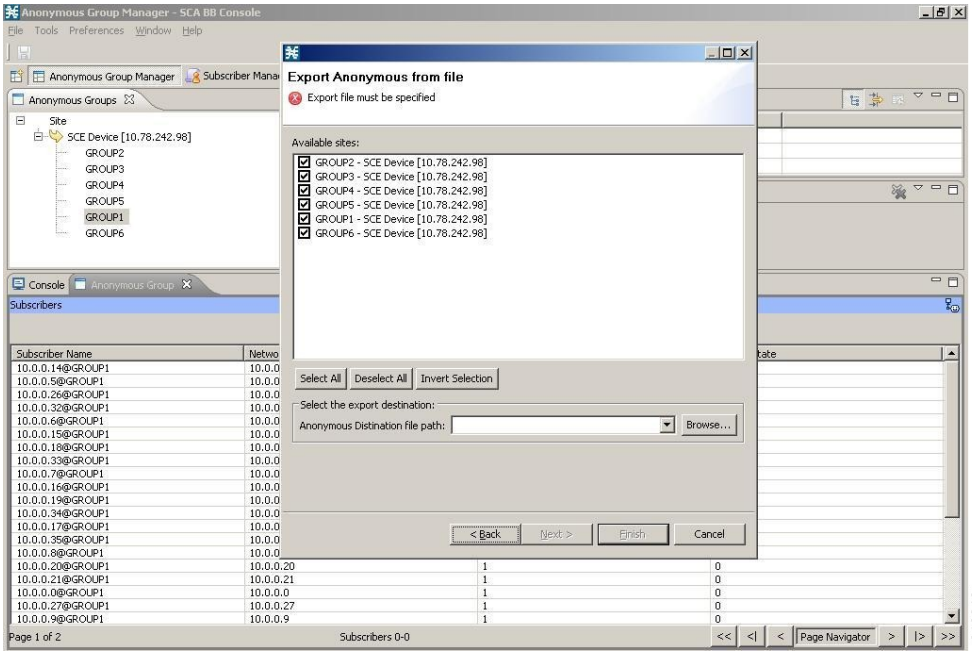
Step 1 From the Console main menu, choose **Tools** > **Anonymous Group Manager**.
The Anonymous Group Manager tool opens.

Step 2 In the Site list, click the Cisco SCE for which you want to export the Anonymous Groups.

Step 3 Select File > Export.

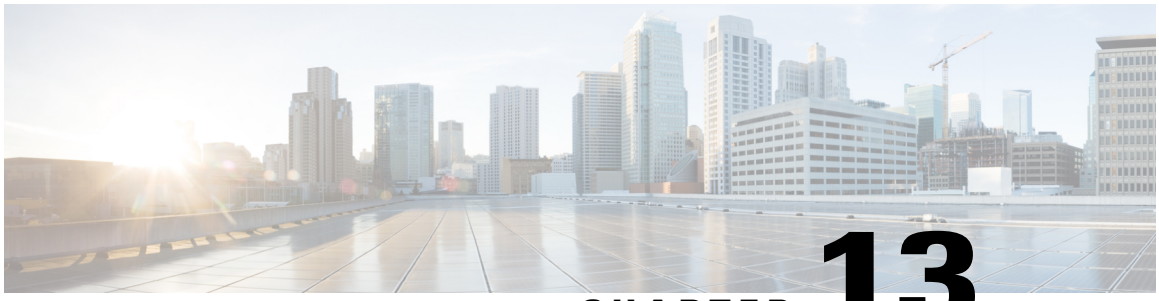
The Export dialog box appears.

Figure 337: Export Dialog Box



Step 4 Select the subscribers to be exported.

Step 5 Select the Export destination and click Finish .
The Export from File dialog box closes. The selected subscriber information is saved to the CSV file.



CHAPTER 13

The Signature Editor Overview

This module describes the Signature Editor tool and how to use it to create and modify Dynamic Signature Script (DSS) files.

The Signature Editor tool allows you to create and modify DSS files that can add and modify protocols and protocol signatures in the Cisco SCA BB, based on your knowledge of new network protocols that Cisco SCA BB is yet to support.

This chapter consists of these sections:

- The Signature Editor Console , page 491
- Managing DSS Files Overview, page 491
- Creating DSS Files , page 502
- Editing DSS Files , page 504
- Importing DSS Files , page 505

The Signature Editor Console

The Signature Editor writes log and error messages to the Signature Editor Console (in the Console view), when appropriate.

Managing DSS Files Overview

- Installing new signatures to an active service configuration is described in Working with Protocol Packs.
- Working with signatures in the Service Configuration Editor is described in Introduction to Managing Protocol Signatures
- Using **servconf,** the Server Configuration Utility, to apply signatures is described in The Cisco SCA BB Service Configuration Utility .

The DSS file components, and the creation and editing of DSS files, are explained in the following sections.

The DSS File Components

The DSS file components are displayed in the Script pane of the Signature Editor, in a tree structure. By selecting the appropriate node of the DSS component tree, you can define the properties associated with the node in the Property pane.

The DSS file components are described in the following sections.

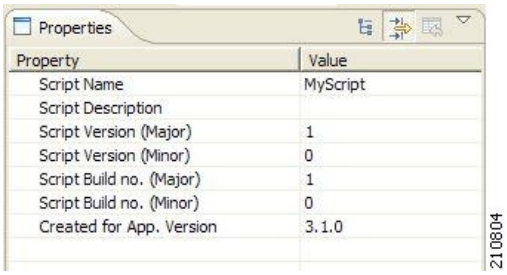
The DSS File

The DSS file name is the root node of the DSS file component tree.

When you select the root node, you can define the following properties for the DSS file:

- Script Name—Enter a meaningful name for this script.
- Script Description—Enter the reason for creating this script and describe its contents.
- Script Version (Major)
- Script Version (Minor)
- Script Build Number (Major)
- Script Build Number (Minor)
- Created for Application Version—Select from a list of predefined values.

Figure 338: Default Values for DSS File Properties



The DSS file contains a single protocol list.

DSS Protocol List

The protocol list has no properties to define. It contains all the protocols that are being added, modified, or enhanced.

Information About DSS Protocols

When you select a Protocol node in the DSS file component tree, you can define the following properties of the protocol:

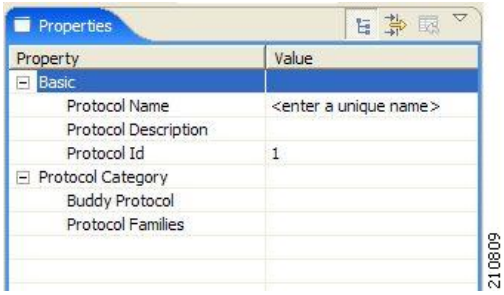
- Basic:

- Protocol Name—See the “Setting Protocol Name and ID” section.
- Protocol Description
- Protocol ID—See the “Setting Protocol Name and ID” section.

- Protocol Category:
  - Buddy Protocol—See “The Buddy Protocol” section.
  - Protocol Families—Assign the protocol to one or more protocol families:
  - P2P
  - SIP
  - VOIP
  - Worm

Associating a protocol with a protocol family allows reports about the family to include the new protocol.

Figure 339: Default Values for the Protocol Properties



Protocols contain signatures.

DSS Protocol Name and ID

A DSS can include two types of protocols:

- A protocol new to Cisco SCA BB—The protocol is being defined in the DSS.
- A protocol that Cisco SCA BB already supports—The protocol identification is being enhanced or modified in the DSS.

Selecting a name and ID is different for the two cases:

- For a protocol new to Cisco SCA BB, the name must not match any of the protocol names that Cisco SCA BB already supports. To see a list of supported-protocol names, open the Protocol Settings dialog box in the Service Configuration Editor (see “How to View Protocols” section). Assign the protocol a unique ID in the range from 5000 to 9998.
- For an existing protocol, the protocol name and ID in the DSS must be identical to the protocol name and ID in the service configuration. Locate the name and ID in the Protocol Settings dialog box in the Service Configuration Editor (see “How to View Protocols” section).

DSS Buddy Protocol

To simplify the configuration of new protocols added by a DSS, the DSS may specify a Buddy Protocol for a new protocol. If, when importing a DSS to a service configuration, the application encounters service elements referring to the Buddy Protocol, it automatically duplicates the set of service elements that use the Buddy Protocol and replaces all references to the Buddy Protocol with references to the new protocol. The association of the new protocol to services matches that of the Buddy Protocol.

DSS Signatures

A protocol may contain as many different signatures as necessary.

Four different types of signatures may be added to a protocol:

- String Match Signatures
- Payload Length Signatures
- HTTP User Agent Signatures
- HTTP x-Header Signatures

Each of the four signature types tests different conditions against the first payload packet of the flows.

These signature types and their conditions are described in the following subsections.

String Match Signatures and Payload Length Signatures can contain deep inspection clauses. A signature whose first payload packet conditions are met accepts a flow if the conditions of any of its deep inspection clauses are also met.

DSS String Match Signature

When you select a String Match Signature node in the DSS file component tree, you can define the following properties of the signature:

- Signature Name—A unique name
- Signature Description
- Signature ID—A value in the range from 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
- First Payload Packet Conditions:
    - Fixed Size Byte String—(Display only) Shows the string formed by the next four fields:
        - [0]—Enter the ASCII code for the first byte of the string, or enter "*" to indicate that any value is acceptable.
        - [1]—Enter the ASCII code for the second byte of the string, or enter "*" to indicate that any value is acceptable.
        - [2]—Enter the ASCII code for the third byte of the string, or enter "*" to indicate that any value is acceptable.
        - [3]—Enter the ASCII code for the fourth byte of the string, or enter "*" to indicate that any value is acceptable.

- String Position—The position of the Fixed Size Byte String in the packet. The position is the location of the first byte of the string, counting from the first byte in the packet. To match the string with the beginning of the packet, this value should be zero. The value must be an integer divisible by four.
- Packet Direction—The initiating side of the first packet in the flow that has a payload. This field can have one of three values:
  - From Server
  - From Client
  - Don't Care (either side)
- Port Range—(Display only) The port range formed by the next two fields. The default value is the entire port range from 0 to 65535.
- From Port—Lower bound of the port range (inclusive)
- To Port—Upper bound of the port range (inclusive)
- Check before PL—Toggles between the values true and false .

This field indicates whether to test the signature before or after the execution of the Cisco SCA BB built-in PL (Protocol Library) classification. Testing this signature before the execution of the built-in classification means that if the flow matches this signature, the PL classification is skipped. If this field is set to "false", this signature is tested only if the PL classification fails to identify any of its supported protocol signatures.

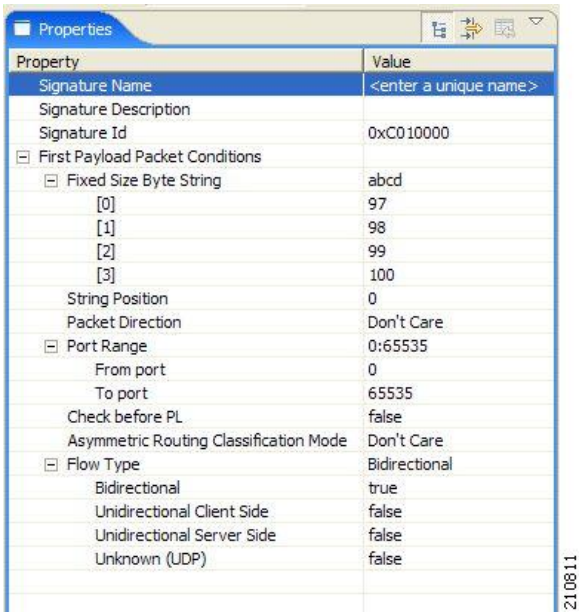
- Asymmetric Routing Classification Mode—This field indicates whether to test the signature depending on the state of the asymmetric routing classification mode. It can have one of three values:
- Don't Care—Signifies that this signature should be tested whether asymmetric routing classification mode is enabled or disabled.
- Disabled
- Enabled
- Flow Type—(Display only) This field shows to which flow types the condition applies (the condition may be applied to multiple types). It is ignored unless asymmetric routing classification mode is enabled.

The next four fields specify the flow type:

- Bidirectional—Toggles between the values true and false .
- Unidirectional Client Side—Toggles between the values true and false . Applies to TCP flows for which only packets from the client side have been detected.
- Unidirectional Server Side—Toggles between the values true and false . Applies to TCP flows for which only packets from the server side have been detected.
- Unknown (UDP)—Toggles between the values true and false . Applies to UDP flows for which packets from only one direction have been detected.

Note Set Check before PL to true only if the signature identifies the protocol according to the first payload packet only. If the signature also uses a Deep Inspection Condition that looks into later packets, and the signature does not match the flow, the PL classification is not performed properly.

Figure 340: Default Values for the String Match Signature Properties



A flow that matches the first payload packet conditions of a String Match Signature is then compared against the deep inspection conditions of the signature (see “DSS Deep Inspection Conditions” section).

DSS Payload Length Signature

When you select a Payload Length Signature node in the DSS file component tree, you can define the following properties of the signature:

- Signature Name—A unique name
- Signature Description
- Signature ID—A value in the range from 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
- First Payload Packet Conditions:
  - Packet Direction—The initiating side of the first packet in the flow that has a payload. This field can have one of three values:
  - From Server
  - From Client
  - Don’t Care (either side)
  - Payload Length—The number of bytes in the payload packet.

- Port Range—(Display only) The port range formed by the next two fields. The default value is the entire port range from 0 to 65535.
- From Port—Lower bound of the port range (inclusive)
- To Port—Upper bound of the port range (inclusive)
- Check before PL—Toggles between the values true and false .

This field indicates whether to test the signature before or after the execution of the Cisco SCA BB built-in PL (Protocol Library) classification. Testing this signature before the execution of the built-in classification means that if the flow matches this signature, the PL classification is skipped. If this field is set to “false”, this signature is tested only if the PL classification fails to identify any of its supported protocol signatures.

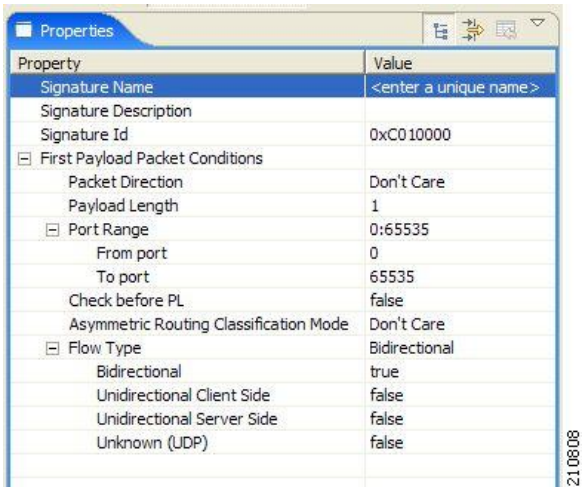
- Asymmetric Routing Classification Mode—This field indicates whether to test the signature depending on the state of the asymmetric routing classification mode. It can have one of three values:
- Don't Care—Signifies that this signature should be tested whether asymmetric routing classification mode is enabled or disabled.
- Disabled
- Enabled
- Flow Type—(Display only) This field shows to which flow types the condition applies (the condition may be applied to multiple types). It is ignored unless asymmetric routing classification mode is enabled.

The next four fields specify the flow type:

- Bidirectional—Toggles between the values true and false .
- Unidirectional Client Side—Toggles between the values true and false . Applies to TCP flows for which only packets from the client side have been detected.
- Unidirectional Server Side—Toggles between the values true and false . Applies to TCP flows for which only packets from the server side have been detected.
- Unknown (UDP)—Toggles between the values true and false . Applies to UDP flows for which packets from only one direction have been detected.

Note Set Check before PL to true only if the signature identifies the protocol according to the first payload packet only. If the signature also uses a Deep Inspection Condition that looks into later packets, and the signature does not match the flow, the PL classification is not performed properly.

Figure 341: Default Values for the Payload Length Signature Properties



A flow that matches the first payload packet conditions of a Payload Length Signature is then compared against the deep inspection conditions of the signature (see “DSS Deep Inspection Conditions” section).

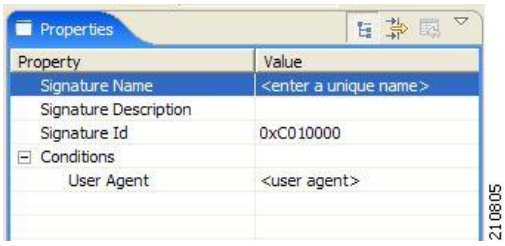
DSS HTTP User Agent Signature

When you select an HTTP User Agent Signature node in the DSS file component tree, you can define the following properties of the signature:

- Signature Name—A unique name
- Signature Description
- Signature ID—A value in the range from 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
- Conditions:

- User Agent—The value of the User Agent field in the HTTP header

Figure 342: Default Values for the HTTP User Agent Signature Properties

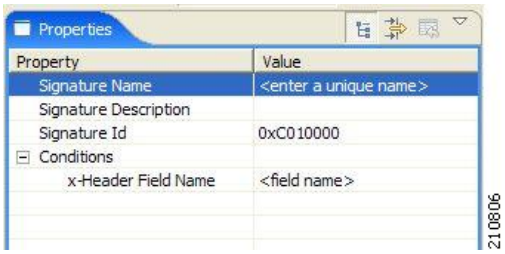


DSS HTTP x-Header Signature

When you select an HTTP x-Header Signature node in the DSS file component tree, you can define the following properties of the signature:

- Signature Name—A unique name
- Signature Description
- Signature ID—A value in the range from 0xC010000 to 0xC0100FF (decimal 201392128 to 201392383)
- Conditions:
  - x-Header Field Name—A name of a field in the x-Header of the HTTP header

Figure 343: Default Values for the DSS File Properties



DSS Deep Inspection Clauses

A deep inspection clause is a conjunctive clause of deep inspection conditions—a signature accepts a flow *only* if all conditions in a clause are met.

Note If a signature has multiple deep inspection clauses, the clauses (and the deep inspection conditions making up each clause) are tested in an order based on the value of the Packet Number property of the deep inspection conditions. After the first payload packet is accepted by the first payload packet conditions, the clause containing the condition with the lowest Packet Number is tested. The other conditions in this clause are checked in ascending Packet Number order. Thus, the Packet Number of any condition in a clause cannot be less than the largest Packet Number in the clause it succeeds.

DSS Deep Inspection Conditions

A deep inspection condition is a set of conditions that are checked against flows that pass the first payload packet conditions screening of String Match Signatures or Payload Length Signatures.

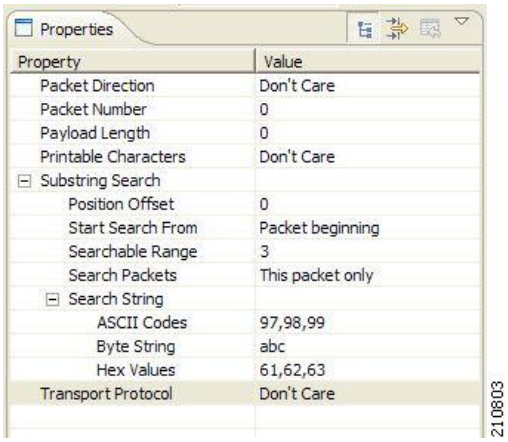
When you select a Deep Inspection Condition node in the DSS file component tree, you can define the following properties of the deep inspection condition:

- Packet Direction—The initiating side of the first packet in the flow that has a payload. This field can have one of three values:
  - From Server
  - From Client
  - Don't Care (either side)
- Packet Number—The number of the packet in the flow. The payload packets are numbered from zero; packets are counted in both directions.
- Payload Length—The length of the packet in bytes. Enter zero to indicate that any value is acceptable.
- Printable Characters—Test if the inspected packet contains only printable characters. This field can have one of three values:
  - Printable Characters Only
  - At Least One Non-Printable
  - Don't Care
- Substring Search—Match a search string with a specific location in the packet. Leave the Search String fields empty if this condition is irrelevant.
  - Position Offset—The position from which to start searching for the search string in the packet. The offset is relative to the location specified in the Start Search From field.
  - Start Search From—This field can have one of two values:
  - Packet beginning
  - Last match

  Last match means that the search for this search string starts where the last search match ended. The last match may be from a previous substring search or from the last string-based first payload packet condition.
- Searchable Range—Search in this number of bytes for the search string.

- Search Packets—This field can have one of two values:
- This packet only
- Multiple packets—
  Multiple Packets means that the search may span across packets, as long as the overall number of bytes is less than the number specified in the Searchable Range field.
- Search String—Enter the search string in one of the following three fields (the other two fields are updated automatically):
  - ASCII Codes—Enter the ASCII codes for the characters of the search string. Separate each code by a comma.
  - Byte String—Enter the actual search string.
  - Hex Values—Enter the hexadecimal values of the ASCII codes for the characters of the search string. Separate each code by a comma.
- Transport Protocol—This field can have one of three values:
  - TCP
  - UDP
  - Don't Care (either TCP or UDP)

Figure 344: Default Values for the Deep Inspection Condition Properties



The structure of deep inspection conditions is the same for String Match Signatures and Payload Length Signatures.

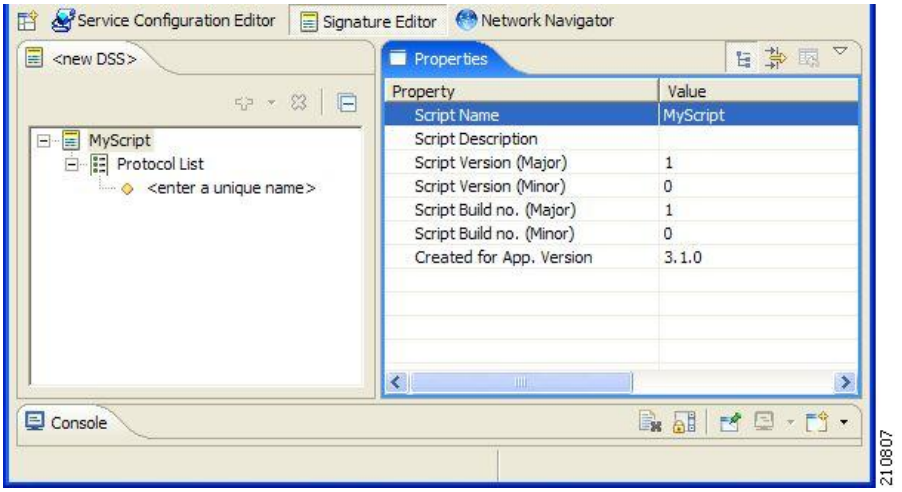
Creating DSS Files

Note If you have a DSS file open in the Signature Editor, save it before you create a new DSS file. All unsaved changes are lost.

Procedure

Step 1 From the toolbar, click the Create a New DSS File ( ) icon.
A DSS component tree containing a DSS File node, a Protocol List node, and a Protocol node, is displayed in the Script view. The default properties of the new DSS file are displayed in the Properties view.

Figure 345: Properties Tab



Step 2 Edit the DSS file properties.
For an explanation of the properties, see “The DSS File” section.

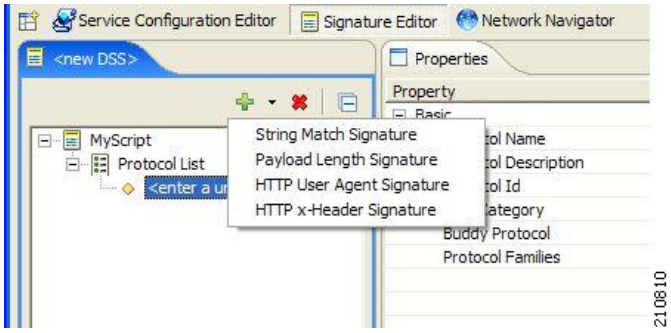
Step 3 Click the Protocol node.
The protocol properties appear in the Properties view.

Step 4 Edit the protocol properties.

For an explanation of the properties, see “Information About DSS Protocols” section.

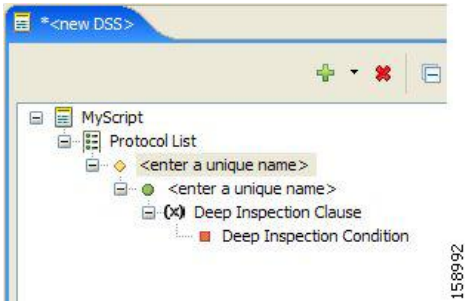
Step 5 Click the drop-down arrow next to the Add ( ) icon.

Figure 346: Protocol Properties



Step 6 From the drop-down menu that appears, select a signature type.
A Signature node is added under the Protocol node. If you selected a String Match Signature or a Payload Length Signature, a Deep Inspection Clause node and a Deep Inspection Condition node are also added.

Figure 347: Protocol List Information



Step 7 Click the Signature node.
The signature properties appear in the Properties view.

Step 8 Edit the signature properties.
For an explanation of the properties, see “DSS Signatures” section.

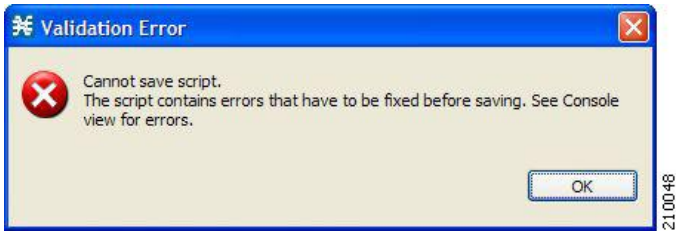
Step 9 If you selected a String Match Signature or a Payload Length Signature, click the Deep Inspection Condition node to edit the deep inspection condition properties.
For an explanation of the properties, see “DSS Deep Inspection Conditions” section.
The deep inspection condition properties appear in the Properties view.

Step 10 Add additional deep inspection conditions, deep inspection clauses, signatures, and protocols as needed.

Step 11 From the toolbar, click the Save ( ) icon.

If there are duplicate protocol names or protocol IDs, a Validation Error message appears.

Figure 348: Validation Error



Step 12 Click OK, remove the duplication, and then click the Save ( ) icon again.
A Save As dialog box appears.

Step 13 Browse to the folder where you want to save the new DSS file.

Step 14 In the File name field, enter an appropriate name for the DSS file.

Step 15 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.

Note If you have a DSS file open in the Signature Editor, save it before you open a different DSS file. All unsaved changes are lost.

Procedure

Step 1 From the toolbar, click the Open a DSS File ( ) icon.

Step 2 Browse to the DSS file that you want to edit.

Step 3 Click Open.
The Open dialog box closes.

The DSS Component tree of the selected file is displayed in the Script view.

The DSS File node is selected, and the properties of the DSS file are displayed in the Properties view.

Step 4 Add, edit, or delete DSS file components.
See the subsections of The DSS File Components section for an explanation of the properties of the different components.

Step 5 Save the modified DSS file.

Step 6 To overwrite the current DSS file with the changes you have made, from the toolbar, click the Save () icon.

Step 7 To save the modified DSS file with a new name choose **File** > **Save As**.

a) Browse to the folder where you want to save the new DSS file.
b) In the File name field, enter an appropriate name for the DSS file.
c) Click **Save**.
The modified DSS file is saved with the new name.

Importing DSS Files

You can import DSS files into the file you are currently editing.



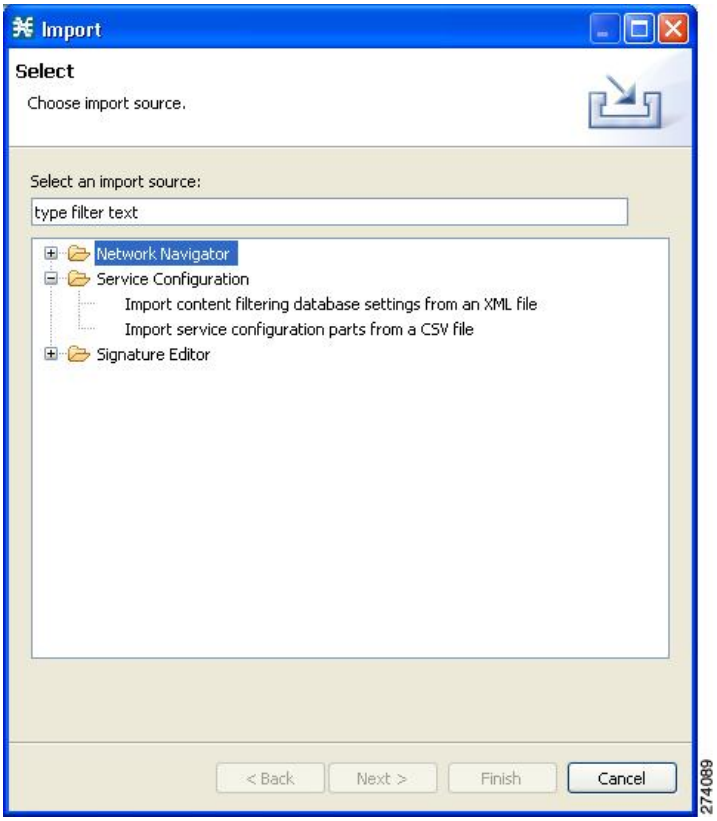
Note Importing signatures may create duplication of protocol names or protocol IDs.

Procedure

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

The Import dialog box appears.

Figure 349: Import

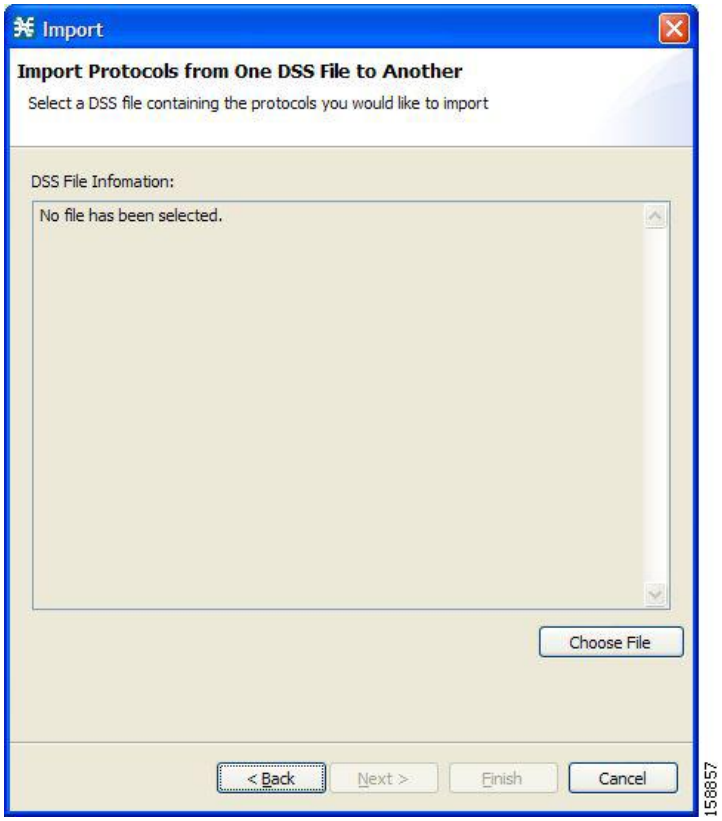


Step 2 From the import source list, select Import protocols from one DSS file to another DSS .

Step 3 Click Next.

The second screen of the Import dialog box opens.

Figure 350: Import Protocols from One DSS File to Another



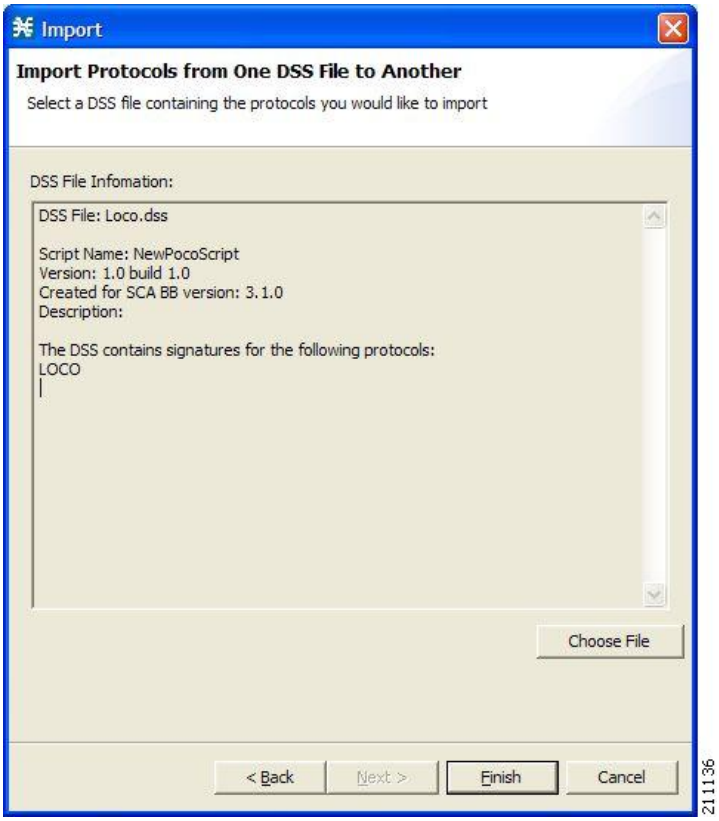
Step 4 Click Choose File.
An Open dialog box appears.

Step 5 Browse to the DSS file to import.

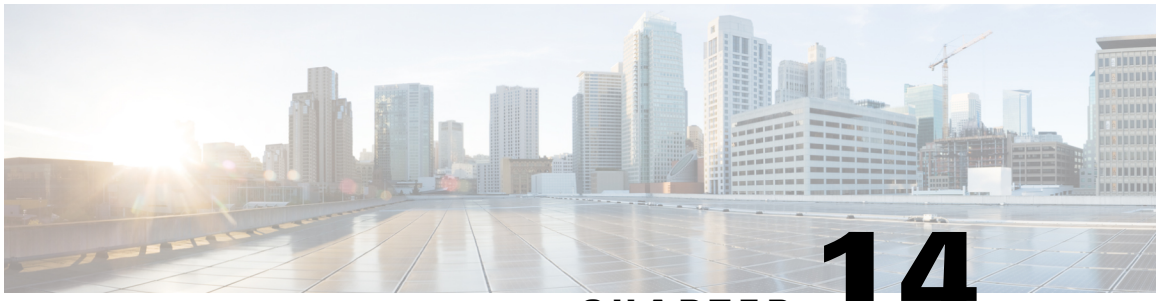
Step 6 Click Open.
The Open dialog box closes.

Information about the DSS file that you have chosen is displayed in the DSS File Information area.

Figure 351: Import Protocols from One DSS File to Another



Step 7 Click Finish.
The Import dialog box closes. The content of the selected DSS file is imported into the Signature Editor.



CHAPTER 14

Additional Management Tools and Interfaces

This chapter provides details on additional management tools and interfaces available in Cisco Service Control.

- The Cisco SCA BB Service Configuration Utility , page 509
- The Cisco SCA BB Signature Configuration Utility , page 513
- Overview of SNMP, MIB, and Traps , page 514
- Installing a Cisco SCA BB PQI File on a Cisco SCE Platform , page 515
- Overview on Managing Subscribers via Other System Components , page 515

The Cisco SCA BB Service Configuration Utility

The Cisco SCA BB Service Configuration Utility (**servconf)** is a command-line utility (CLU) for applying and retrieving service configurations. Use it in a scripting environment to automate service configuration tasks on multiple Cisco Service Control Engine (Cisco SCE) platforms.

The Service Configuration Utility can run in Windows and Linux environments.

servconf Syntax

The command-line syntax of **servconf** is: **servconf**<*operation*> *[<option>] [<option>] ...*

Table 17: servconf Operations

Operation	Abbreviation	Description
--apply	-a	Copies the specified service configuration file to the specified Cisco SCE platforms and activates it

Operation	Abbreviation	Description
--retrieve	-r	Retrieves the current service configuration
--update-dc	-u	Updates a Cisco Service Control Collection Manager (CM) with service configuration values
--status	—	Shows the service configuration status on the Cisco SCE platform
--update-signature	—	Updates the Cisco SCE platform with a new protocol pack
--update-signature-pqi	—	Updates the Cisco SCE platform with a new SPQI protocol pack
--signature-info	-i	Shows information about the Dynamic Signature Script (DSS) file
--help	—	Displays help, then exits
--version	—	Displays the program version number, then exits

Table 18: servconf File Options

File Option	Abbreviation	Description
--file= *filename*	-f	Specifies a service configuration file or DSS file
--backup-directory= *directory*	-b	Specifies the directory to which to save the retrieved PQB file before applying a new protocol pack

Table 19: servconf Connection Options

File Option	Abbreviation	Description
--se= *address*	-S	Specifies the IP address of the destination Cisco SCE platform. To specify multiple Cisco SCE platforms, list the IP addresses separated by semicolons (see Example 1 in the following section). When using a semicolon in a Unix command line, the command-line argument must be enclosed in quotation marks.
--dc= *address*	-D	Specifies the IP address of the destination Cisco Service Control Collection Manager platform (required only for the --update-dc operation).
--password= *password*	-P	Specifies the password for connecting to the Cisco SCE platform.
--username= *username*	-U	Specifies the username for connecting to the Cisco SCE platform. If this option is not specified, the following default values are used: • SCE—admin • CM—pcube • SM—pcube

Table 20: servconf Reference Cisco SCE Option

File Option	Description
--refer-se= *address*	Specifies the IP address of the Cisco SCE platform to which the service configuration values refer (required only for --update-dc operation)

Table 21: servconf Apply Options

File Option	Description
--no-dc	(Optional) Specifies that the --apply operation should not automatically update the Cisco Service Control Collection Manager with service configuration values.
--no-default-signature	Applies the service configuration without adding the default DSS to it.
--force-default-signature	Forces the replacement of the DSS in the retrieved PQB with the default DSS, even if the signatures of the existing DSS are mapped to services. Without this flag, trying to update a PQB containing a DSS fails.

Table 22: servconf Update Signature Option

File Option	Description
--force-signature	Forces replacement of the DSS in the retrieved PQB, even if the signatures of the existing DSS are mapped to services. Without this flag, trying to update a PQB containing a DSS fails.

servconf Examples

Example 1

To copy the service configuration file config.pqb from the local machine to two Cisco SCE platforms (at 63.111.106.7 and 63.111.106.12), and activate this configuration:

```
servconf "--se=63.111.106.7;63.111.106.12" --username Alice --password ***** --apply
                --file config.pqb
```

Example 2

To retrieve the current service configuration from the Cisco SCE platform at 63.111.106.7, and save it in file my_files\config.pqb on the local machine:

```
servconf -S 63.111.106.7 -U Bob -P ***** --retrieve --file my_files\config.pqb
```

Example 3

To update the Cisco Service Control Collection Manager at 63.121.116.17 with service configuration values from file config.pqb, as if they were applied to the Cisco SCE platform at 63.111.106.7 (but without actually applying them to the Cisco SCE platform):

```
servconf -D 63.121.116.17 -U Alice -P ***** --update-dc --refer-se 63.111.106.7
                --file config.pqb
```

Example 4

To distribute the protocol pack file new_signature.spqi to the Cisco SCE platforms at 10.56.216.33 and 10.56.216.36:

```
servconf --update-signature-pqi -f new_signature.spqi -S "10.56.216.33;10.56.216.36"
                -U user123 -P *****
```

The Cisco SCA BB Signature Configuration Utility

The Cisco SCA BB Signature Configuration Utility (**sigconf)** is a command-line utility for installing and managing the default DSS.

The Signature Configuration Utility can run in Windows and Linux environments.

For installation instructions, see Installing the Cisco SCA BB Configuration Utilities .

sigconf Syntax

The command-line syntax of the Cisco SCA BB Signature Configuration Utility is **sigconf** <*operation*> [**--file** <*filename*>]

Table 23: sigconf Operations

Operation	Abbreviation	Description
--set-default-dynamic-signature	-d	Installs the default DSS on this workstation.
--remove-default-dynamic-signature	—	Uninstalls the default DSS from this workstation.
--get-default-dynamic-signature	—	Fetches the default DSS installed on this workstation.
--help	—	Displays help, then exits.

Table 24: sigconf File Option

File Option	Abbreviation	Description
--file *filename*	-f	Specifies a DSS file

sigconf Examples

Example 1

To install the file new_signature.dss as the default DSS:

sigconf --set-default-dynamic-signature --file new_signature.dss

Example 2

To retrieve the installed default DSS file, and save it as default_backup.dss:

sigconf --get-default-dynamic-signature --file default_backup.dss

Overview of SNMP, MIB, and Traps

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

Two interfaces are provided for network management:

- Command-line interface (CLI)—Accessible through the console port on the front panel of the Cisco SCE platform or through a Telnet connection to the Cisco SCE platform, the CLI is used for configuration and security functions.
- SNMP (Simple Network Management Protocol)—Provides fault management (via SNMP traps) and performance monitoring functionality.

SNMP

SNMP is a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

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 Cisco SCE platform supports the following MIBs:

- MIB-II—Defined in RFC 1213, (Management Information Base for Network Management of TCP/IP-based Internets)
- Cisco Service Control Enterprise MIB—Described by a number of MIB files

The Cisco proprietary MIB allows external management systems to retrieve general information about the Cisco SCE platform operating status and resource utilization, extract real-time measurements of bandwidth utilization and network statistics, and receive notifications of critical events and alarms.

Traps

Traps are unsolicited messages generated by the SNMP agent that resides inside the Cisco 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 Cisco SCE platform supports two general categories of traps:

- Standard SNMP traps—As defined in RFC 1157 and using the conventions defined in RFC 1215
- Proprietary Cisco Service Control Enterprise traps—As defined in the Cisco proprietary MIB

Installing a Cisco SCA BB PQI File on a Cisco SCE Platform

You can install a Cisco SCA BB PQI file on a Cisco SCE platform using the Cisco SCE platform Command-Line Interface (CLI).

Procedure

Step 1 Make sure that the PQI file is available.
Do one of the following:

- Locate the PQI file on the Cisco SCE platform.
- Upload the appropriate PQI file to the Cisco SCE via FTP.

Step 2 Enter line interface configuration mode.

Step 3 Type **pqi install file engXXXXX.pqi** .

Step 4 Monitor the installation progress until it is completed.
After you install the Console, you can use the Network Navigator tool to install PQI files. See the Installing PQI Files on Cisco SCE Devices , on page 126 section.

Entering Line Interface Configuration Mode

Procedure

Step 1 At the Cisco SCE platform CLI prompt (SCE#), type **configure** and press Enter.
The SCE(config)# prompt appears.

Step 2 Type **interface LineCard 0** .

Step 3 Press **Enter**.
The SCE(config if)# prompt appears.

Overview on Managing Subscribers via Other System Components

Other components of the Cisco Service Control solution offer alternatives for subscriber management (as opposed to using the Subscriber Manager GUI tool in the Console):

- The Cisco Service Control Subscriber Manager (SM) has options that are not available from the Console.
- The Cisco SCE platform has a wide range of subscriber-related functions.

For in-depth explanations, see the appropriate Service Control documentation.

This section gives an overview of these alternatives, with emphasis on the Cisco SCA BB-specific subscriber management options:

- Anonymous Subscriber Mode
- Subscriber-Aware Mode
- Selecting Subscribers for Real-Time Usage Monitoring
- Managing Subscriber CSV Files

Anonymous Subscriber Mode

An anonymous subscriber is one with a name generated automatically by the Cisco SCE platform according to an anonymous subscriber group specification. An anonymous subscriber is always mapped to a single IP address. The actual identity of the customer is unknown to the system.

An anonymous group is a specified IP range, possibly assigned a subscriber template. If an anonymous group is configured, the Cisco SCE platform generates anonymous subscribers for that group when it detects traffic with an IP address in the specified IP range. If a subscriber template is assigned to the group, the anonymous subscribers generated have properties defined by that template. If no subscriber template is assigned, the default template is used, which cannot be changed by template import operations. Initially, 200 templates are preconfigured, one for each package ID.

Anonymous subscriber groups and subscriber templates are managed using the Cisco SCE platform Command-Line Interface (CLI). You can enter CLI commands via a Telnet session. For more information, see the or .

Use the following commands to import anonymous subscriber groups and subscriber templates from CSV files and to export subscriber data to these files:

- subscriber anonymous-group import csv-file
- subscriber anonymous-group export csv-file
- subscriber template import csv-file
- subscriber template export csv-file



Note The preceding CLI commands are line interface configuration commands. You must enter line interface configuration mode (see Entering Line Interface Configuration Mode , on page 515 section) and see the SCE(config if)# prompt displayed before entering a command.

Use the following commands to delete anonymous groups or subscriber templates from the system.

- no subscriber anonymous-group [all] [name <groupname>]
- clear subscriber anonymous
- default subscriber template all

Note The preceding CLI commands are line interface configuration commands. You must enter line interface configuration mode (see Entering Line Interface Configuration Mode , on page 515 section) and see the SCE(config if)# prompt displayed before entering a command.

Use the following commands to display anonymous subscriber information:

- show interface LineCard 0 subscriber templates [index]
- show interface LineCard 0 subscriber anonymous-group [all] [name <groupname>]
- show interface LineCard 0 subscriber amount anonymous [name <groupname>]
- show interface LineCard 0 subscriber anonymous [name <groupname>]

Subscriber-Aware Mode

In subscriber-aware mode, each subscriber is a specific customer with an externally generated name. This externally generated name allows the subscriber to be mapped to more than one IP address and still be identified. Each traffic session (single IP flow, or a group of related IP flows) processed by the Cisco SCE platform is assigned to a recognized subscriber on the basis of the configured subscriber mappings.

There are three options for introducing and managing these subscribers:

- The SM GUI tool (see Subscriber Manager GUI Tool Overview, on page 457 section)

The Cisco SCE Platform Subscriber CLI

Use the following commands to import subscriber data from CSV files and to export subscriber data to these files:

subscriber import csv-file

subscriber export csv-file

Note The preceding CLI commands are line interface configuration commands. You must enter line interface configuration mode (see Entering Line Interface Configuration Mode , on page 515 section) and see the SCE(config if)# prompt displayed before entering a command.

Use the following command to remove subscribers from the system.

no subscriber [all] [name <subscriber-name>]

Note The preceding CLI command is a line interface configuration command. You must enter line interface configuration mode (see Entering Line Interface Configuration Mode , on page 515) and see the SCE(config if)# prompt displayed before entering the command.

Use the following commands to display subscribers meeting various criteria:

show interface LineCard 0 subscriber [amount] [prefix <prefix>] [property <propertyname> equals | greater-than | less-than <property-val>]

show interface LineCard 0 subscriber [amount] prefix <prefix>

show interface LineCard 0 subscriber [amount] suffix <suffix>

show interface LineCard 0 subscriber mapping IP <iprange>

show interface LineCard 0 subscriber [amount] mapping intersecting IP <iprange>

show interface LineCard 0 subscriber mapping VLANid <vlanid>

Use the following commands to display information about a specific subscriber:

show interface LineCard 0 subscriber properties

show interface LineCard 0 subscriber name <name>

show interface LineCard 0 subscriber name <name> mappings

show interface LineCard 0 subscriber name <name> counters

show interface LineCard 0 subscriber name <name> properties

The SM Subscriber Management CLU

The SM Subscriber Management Utility (**p3subs)** is a CLU for managing subscribers. You can use it to add or remove subscribers. You can also manage subscriber properties and mappings with this utility.

For more information about **p3subs,** see the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

p3subs Syntax

You run **p3subs** from the Solaris shell prompt. The command-line syntax of the utility is:

p3subs <*operation*> **--subscriber**=<*Subscriber-Name*> [**--ip**=<*IP-address*>] [**--property**=<*property-name=value*>] [**--domain**=<*domain-name*>] [**--overwrite**]

The following table lists the **p3subs** operations relevant to managing subscribers.

Table 25: p3subs Subscriber Operations to Manage Subscribers

Operation	Description
--add	Adds a subscriber or replaces the existing subscriber configuration
--set	Updates mappings and properties for the specified subscriber
--remove	Removes the specified subscriber
--show	Displays information for specified subscriber

Selecting Subscribers for Real-Time Usage Monitoring

Real-Time Subscriber Usage RDRs report the network activity of a single subscriber per service per metric, in real-time. You must enable the generation of these subscriber usage RDRs separately for each subscriber that you wish to monitor.



Note Generating and collecting Real-Time Subscriber Usage RDRs for many subscribers can compromise performance. Enable Real-Time Subscriber Usage RDR generation only for subscribers that must be monitored.

The monitor subscriber property controls the generation of Real-Time Subscriber Usage RDRs. By default, generation of these RDRs is disabled (monitor = 0). To enable generation of the RDRs, change the value of the property to 1.

You can modify this property for selected subscribers using either the SM Command-Line Utility (CLU) or the Cisco SCE platform CLI.

This section explains the following procedures:

Managing Subscriber Monitoring via the SM

You can enable or disable the generation of the Real-Time Subscriber Usage RDRs using the SM **p3subs** utility. You can also create a file that processes a batch of subscribers. For more information, see the *Cisco Service Control Management Suite Subscriber Manager User Guide.*

Enabling Subscriber Monitoring for a Subscriber via the SM

You can enable subscriber monitoring for a specified subscriber.

Procedure

From the command line, run **ssm/server/bin/p3subs --set --subscriber Smith --property monitor=1.**

Disabling Subscriber Monitoring for a Subscriber via the SM

Procedure

From the command line, enter **sm/server/bin/p3subs --set --subscriber Smith --property monitor=0.**

Enabling Subscriber Monitoring for Multiple Subscribers

You can enable subscriber monitoring for multiple subscribers.

Procedure

Step 1 Create a text file (named monitor.txt in this example) containing the sequence of CLI invocations, including the commands to access the appropriate CLI mode.

The file would look something like this:

```
configure
        interface LineCard 0
        subscriber name Jerry property name monitor value 1
        subscriber name George property name monitor value 1
        subscriber name Elaine property name monitor value 1
        subscriber name Kramer property name monitor value 1
        subscriber name Newman property name monitor value 1
```

Step 2 From the Cisco SCE platform CLI prompt (SCE#), run **script run monitor.txt**

Verifying that Subscriber Monitoring is Enabled for a Subscriber via the SM

Procedure

From the command line, run **sm/server/bin/p3subs --show-property --subscriber Smith --property monitor.**

Managing Subscriber Monitoring via the Cisco SCE Platform Overview

You can also enable or disable the generation of the Real-Time Subscriber Usage RDRs using the Cisco SCE platform. For more information this, see the

This section explains the following procedures:

Enabling Subscriber Monitoring for a Subscriber

You can enable subscriber monitoring for a specified subscriber.

Procedure

Step 1 Enter line interface configuration mode. (See " Entering Line Interface Configuration Mode " section.)

Step 2 At the SCE(config if)# prompt, run **subscriber name Smith property name monitor value 1.**

Disabling Subscriber Monitoring for a Subscriber

Procedure

Step 1 Enter line interface configuration mode. (See " Entering Line Interface Configuration Mode " section.)

Step 2 At the SCE(config if)# prompt, enter **subscriber name Smith property name monitor value 0.**

Enabling Subscriber Monitoring for Multiple Subscribers

You can enable subscriber monitoring for multiple subscribers.

Procedure

Step 1 Create a text file (named monitor.txt in this example) containing the sequence of CLI invocations, including the commands to access the appropriate CLI mode.
The file would look something like this:

```
configure
        interface LineCard 0
        subscriber name Jerry property name monitor value 1
        subscriber name George property name monitor value 1
        subscriber name Elaine property name monitor value 1
        subscriber name Kramer property name monitor value 1
        subscriber name Newman property name monitor value 1
```

Step 2 From the Cisco SCE platform CLI prompt (SCE#), run **script run monitor.txt**

Verifying that Subscriber Monitoring is Enabled for a Subscriber

Procedure

From the Cisco SCE platform CLI prompt (SCE#), run **show interface LineCard 0 subscriber name Smith properties.**
The properties are displayed; *monitor* is the relevant parameter.

```
Subscriber smith properties:
subscriberPackage=0
monitor=1
Subscriber 'smith' read-only properties
```

Managing Subscriber CSV Files

Use the **p3subsdb** SM utility to import and export subscriber CSV files. You can import subscriber information for a group of subscribers from a CSV file into the SM database. You can also export subscriber information from the SM database to a CSV file.

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

CSV file structure is described in the "CSV File Formats" chapter of *Cisco Service Control Application for Broadband Reference Guide.*

This section explains the following procedures:

Importing Subscriber CSV Files

Procedure

At the Solaris shell prompt, run **p3subsdb --import <filename>.**

Exporting Subscriber CSV Files

Procedure

At the Solaris shell prompt, run **p3subsdb --export <filename>** .

Filtering and Exporting Subscribers Example

The following example exports every subscriber whose name begins with ‘a’ to the file silverSubscriberFile.csv

p3subsdb --export --prefix=a -–output=silverSubscriberFile.csv