



Cisco ECDS 2.5 Software Administration Guide and Online Help

September 2012

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Guide on Cisco.com.

Americas Headquarters

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

Text Part Number: OL-24531-01

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Cisco ECDS 2.5 Software Administration Guide
© 2011-2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xvii

What's in This Guide	xvii
Audience	xvii
Document Revision History	xviii
Document Organization	xviii
Document Conventions	xx
Related Documentation	xxi
Obtaining Documentation and Submitting a Service Request	xxi

CHAPTER 1

Product Overview 1-1

What is Cisco ECDS	1-1
How Cisco ECDS Works	1-3
Ingest and Distribution	1-4
Prefetch Ingest	1-4
Dynamic Ingest	1-4
Hybrid Ingest	1-5
Live Stream Ingest and Split	1-5
Delivery	1-5
Request Routing	1-5
Management	1-6
Content Delivery System Architecture	1-6
Service Engine	1-7
Content Acquirer	1-7
Media Streamer	1-8
Service Router	1-21
Request Routing Engine	1-21
Proximity Engine	1-28
Routing Using WCCP	1-28
Content Delivery System Manager	1-31
Authentication, Authorization, and Accounting	1-31
Device Management	1-31
Delivery Services Management	1-32
Resiliency and Redundancy	1-32
Content Acquirer Redundancy	1-32

Media Streamer Redundancy	1-33
Service Router Redundancy	1-33
Enterprise CDSM Redundancy	1-33
Where to Go Next	1-33

CHAPTER 2

Network Design 2-1

Provisioning the Cisco ECDS	2-1
Cisco ECDS Topology	2-2
Device Groups	2-3
Baseline Groups	2-3
Delivery Service	2-3
Content Acquirer	2-4
Content Acquirer Selection for Prefetched Content	2-4
Content Acquirer Selection for Dynamic or Hybrid Ingest	2-5
Location Leader	2-5
Location Leader Selection for Prefetched Content	2-6
Location Leader Selection for Live Streaming	2-6
Location Leader Selection for Dynamic or Hybrid Content	2-6
Forwarder and Receiver Service Engines	2-6
Persistent HTTP Connections	2-7
Network Partition	2-8
Delivery Service Distribution Tree	2-8
Types of Delivery Services	2-9
Prefetch/Caching Delivery Services	2-9
Live Delivery Service	2-9
Methods for Ingesting Content	2-9
Origin Servers	2-10
Manifest File	2-10
Content Acquirer	2-11
Media Streamer	2-12
Workflow Diagrams	2-12
Content Request Using the Service Router	2-13
Content Request Using WCCP	2-15
WCCP Services	2-15
WCCP Service Negotiation	2-16
WCCP Service Groups	2-16
Dynamic WCCP Redirection Services	2-17
WCCP Custom Web Cache Service	2-17
WCCP Interception	2-17

WCCP Redirection	2-18
WCCP Load Balancing- Source and Destination IP Hash	2-18
Hash Assignment	2-18
Mask Assignment	2-19
Weight Assignment	2-19
WCCP Availability Monitoring	2-19
WCCP Failover	2-19
Multiple Router/Multiple Service Engine Support	2-19
Additional WCCP Support	2-19
TCP Flow Protection	2-20
Slow Start	2-21
Dynamic Service and Port List	2-21
WCCP Transparent Routing Bypass Options	2-21
HTTP and HTTPS Support	2-22
Web Engine HTTP Connections	2-22
IP Spoofing for HTTP	2-23
HTTPS Caching	2-24
Transparent HTTPS Caching Using SSL	2-24
HTTPS Certificates	2-25
HTTPS Service Rules	2-25
HTTPS Requests on Ports	2-25
HTTPS Connection Statistics	2-25
HTTPS Protocol Protection	2-26
Transparent Proxy Support for HTTPS (Live and VoD)	2-26
Programs	2-27
Live Programs	2-27
Rebroadcasts	2-27
API Program File	2-27
Where to Go Next	2-28

CHAPTER 3

Getting Started 3-1

Configuring the Cisco Media Delivery Engines for the First Time	3-1
Logging In to the Enterprise CDSM	3-1
Activating and Synchronizing the Devices	3-3
Activating and Setting NTP for Each Device	3-3
Activating All Inactive Service Engines	3-5
Navigating the Enterprise CDSM	3-6
Devices, Services, and Other Tables	3-7
Devices Home Page	3-8

Task Bar	3-9
Configuring Primary and Standby Enterprise CDSMs	3-11
Changing a Standby to a Primary Enterprise CDSM	3-12
Recovering from Two Primary Enterprise CDSMs	3-13
Typical Configuration Workflow	3-14
Where to Go Next	3-15

CHAPTER 4

Configuring Devices 4-1

Configuring Locations	4-1
Configuring Device Groups	4-3
Working with Device Groups	4-5
Verifying Devices in Device Groups	4-6
Managing New Device Groups	4-6
Managing Aggregate Settings	4-8
Managing Device Group Overlap	4-9
Configuring the Enterprise CDSM	4-9
Where to Go Next	4-10

CHAPTER 5

Configuring the Service Engine 5-1

Activating a Service Engine	5-1
Assigning Devices to Device Groups	5-5
Configuring Bandwidth for Replication and Ingest	5-6
Default Bandwidth	5-7
Scheduled Bandwidth	5-8
Bandwidth Graph	5-10
Service Control	5-11
Configuring Service Rules	5-11
Enabling Service Rules	5-12
Enabling Apple HTTP Live Streaming	5-15
Executing Rule Actions in Order	5-17
Configuring ICAP Services	5-18
Configuring PCMM QoS Policy	5-18
Configuring URL Signing	5-18
Configuring the Authorization Service	5-18
Configuring Transaction Logging	5-19
Application Control	5-22
Configuring Bandwidth	5-22
Configuring Default and Maximum Bandwidth	5-22

Configuring Bandwidth Schedules	5-23
Bandwidth Graph	5-24
Configuring Windows Media Streaming	5-25
Configuring General Settings	5-26
Configuring the Incoming Bandwidth Bypass List	5-31
Configuring Proxy Bypass Lists	5-32
Configuring the Windows Media Outgoing Proxy Bypass List	5-32
WMT Outgoing HTTP Proxy Bypass Commands	5-32
Configuring the Outgoing RTSP Proxy Bypass List	5-33
Configuring Movie Streamer General Settings	5-35
Configuring RTSP Advanced Settings	5-37
Configuring Flash Media Streaming	5-37
Configuring General Settings	5-37
Configuring the FMS Administrator	5-38
Configuring Flash Media Streaming Service Monitoring	5-39
Configuring HTTP	5-39
Configuring Web Engine HTTP Connections	5-39
Configuring the Outgoing Proxy Bypass List	5-42
Configuring Web Engine HTTP Caching	5-43
Configuring Web Engine HTTP Cache Freshness	5-45
Configuring Web Engine Advanced HTTP Caching	5-46
Configuring HTTPS	5-48
Configuring HTTPS Certificates	5-49
Configuring HTTPS Certificate Groups	5-54
Configuring HTTPS Keys	5-57
Configuring HTTPS Servers	5-60
HTTPS Configuration Examples	5-63
General Settings	5-64
Configuring Content Management	5-65
Login Access Control	5-65
Login Authentication	5-66
Configuring SSH	5-68
Enabling Telnet	5-68
Setting the Message of the Day	5-69
Changing the CLI Session Time	5-70
Changing Users—Admin Password	5-70
Creating, Editing, and Deleting Users—Usernames	5-70
Authentication	5-71
Configuring RADIUS Server Settings	5-72
Configuring TACACS+ Server Settings	5-73

Configuring an Access Control List (ACL)	5-74
Scheduling Database Maintenance	5-75
Setting Storage Handling	5-76
Network Settings	5-77
Enabling FTP Services	5-77
Enabling DNS	5-78
Enabling RCP	5-78
Configuring NTP	5-79
Setting the Time Zone	5-79
Viewing Network Interfaces	5-82
Configuring External IP Addresses	5-82
Configuring Port Channel and Load Balancing Settings	5-83
Configuring IP General Settings	5-83
Configuring IP ACL	5-84
Configuring Notification and Tracking	5-95
Enabling Alarm Settings	5-95
Setting Service Monitor Thresholds	5-97
Configuring SNMP	5-100
Supported MIBs	5-106
Enabling System Logs	5-107
Multiple Hosts for System Logging	5-108
Enabling the Kernel Debugger for Troubleshooting	5-109
Configuring Service Router Settings	5-109
Where to Go Next	5-110

CHAPTER 6

Configuring the Service Router 6-1

Activating a Service Router	6-1
Configuring Application Control	6-3
Configuring Last-Resort Routing	6-4
Creating a New Service	6-5
Error File Name Examples	6-6
Creating ASX Error Message Files for Windows Media Live Programs	6-7
Configuring Transaction Logs for the Service Router	6-7
Where to Go Next	6-9

CHAPTER 7

Configuring WCCP 7-1

Configuring WCCP General Settings	7-1
Configuring WCCP Services	7-3
Configuring WCCP Service Settings	7-3

Creating New WCCP Service	7-4
Configuring WCCP Services	7-5
Configuring Dynamic Service Settings	7-6
Configuring Load Balancing Hash	7-6
Configuring Other Settings	7-7
Managing WCCP Service Masks	7-9
Configuring WCCP Service Masks	7-9
Modifying WCCP Service Masks	7-10
Viewing WCCP Service Masks	7-11
Deleting a WCCP Service Mask	7-11
Managing WCCP Router Lists	7-12
Creating WCCP Router Lists	7-12
Modifying WCCP Router Lists	7-13
Viewing WCCP Router Lists	7-14
Managing WCCP Port Lists	7-15
Configuring WCCP Port Lists	7-15
Modifying WCCP Port Lists	7-17
Configuring WCCP Transparent Routing Bypass Settings	7-18
Creating WCCP Bypass List Entries	7-19
Configuring HTTP IP Spoofing with WCCP	7-19
Basic WCCP CLI Configuration Examples	7-21
Enabling WCCP on the Router	7-21
Configuring the Router List Example	7-22
Configuring a Multiple Router/Multiple SE WCCP Service Example	7-22
Configuring WCCP for Flash Media Streaming	7-22
Load Balancing Command Examples	7-22
Hash Assignment Command Example	7-23
Mask Assignment Command Example	7-23
Weight Assignment Command Example	7-24
Web Caching Command Examples	7-24
Web Cache Service Configuration with Clients and Service Engine on the Same Subnet	7-25
Configuring the Service Engine for Web Cache Service—Clients and Service Engine on the Same Subnet	7-25
Configuring the Router for Web Cache Service—Clients and Service Engine on the Same Subnet	7-25
Configuration Examples—Web Cache Service with Clients and Service Engine on the Same Subnet	7-26
Web Cache Service Configuration with Clients and Service Engine on Different Subnets	7-27
Configuring the Service Engine for Web Cache Service—Clients and Service Engine on Different Subnets	7-27

Configuring the Router for Web Cache Service—Clients and Service Engine on Different Subnets	7-27
Configuration Examples—Web Cache Service with Clients and Service Engine on Different Subnets	7-29
Where to Go Next	7-30

CHAPTER 8

Configuring Services 8-1

Configuring Delivery Services	8-1
Content Origins	8-1
Creating Delivery Service	8-4
Create a Service Definition	8-4
Configure General Settings	8-7
Configure Authorization Service	8-8
Configure SE and Content Acquirer Assignment or Device Group and Content Acquirer Assignment	8-8
Identifying Content	8-10
Identifying Content Using the CDSM	8-10
Defining a Crawl Task	8-13
Launching Quick Crawl	8-15
Configuring Advanced Settings	8-16
Configuring Proxy Server Settings	8-19
Identifying Content Using a Manifest File	8-21
Manifest File Proxy Server Settings	8-24
Verifying Content Acquisition	8-25
Configuring Programs	8-25
Defining a Program	8-26
Configuring Live Programs	8-27
Priming a Live Delivery Service	8-32
Configuring a Rebroadcast	8-33
Viewing the Multicast Addresses	8-36
Viewing Programs	8-37
Viewing and Modifying API Programs	8-38
Previewing a Program	8-39
Copying a Program	8-39
Where to Go Next	8-40

CHAPTER 9

Configuring the System 9-1

Configuring AAA	9-1
Creating, Editing, and Deleting Users	9-2

Creating, Editing, and Deleting Roles	9-5
Creating, Editing, and Deleting Domains	9-6
Changing a Password	9-6
Configuring System Settings	9-7
System Properties	9-7
Configuring Fast SE Offline Detection	9-8
Configuring Distribution QoS	9-10
Configuring Service Routing	9-11
Coverage Zone File Registration	9-11
Configuring Global Routing	9-13
Where to Go Next	9-14

CHAPTER 10

Monitoring the Enterprise CDS	10-1
System Monitoring	10-1
System Status	10-1
Device Alarms	10-2
Service Alarms	10-3
System Home Page	10-4
System Audit Logs	10-6
System Port Numbers	10-7
Device Monitoring	10-9
Devices Table	10-9
Devices Home Page	10-11
Using the CDSM Show/Clear Commands Tool	10-12
Show Commands	10-13
Clear Commands	10-21
CPU Utilization	10-22
Viewing Reports	10-22
Report Types	10-22
System Wide Reports	10-23
Location Reports	10-23
Service Engine Reports	10-23
Report Content	10-24
Bandwidth Served	10-24
Bandwidth Efficiency Gain	10-25
Streaming Sessions	10-26
Delivery Service Monitoring	10-27
Delivery Services Table	10-27
Replication Status for a Delivery Service	10-30

Content Replication Status by Delivery Service	10-33
Content Replication Status by Device	10-35
Viewing Statistics	10-37
Viewing Service Engines and Device Group Statistics	10-37
Viewing Routing Statistics	10-39
Viewing Replication States	10-39
Managing Transaction Logs	10-41
Transaction Log Formats for Web Engine	10-42
Extended Squid	10-42
Apache	10-42
Custom Format	10-43
Transaction Logging and NTLM Authentication	10-44
Usage Guidelines for Log Files	10-44
Working Logs	10-44
Archive Working Log	10-45
Exporting Log Files	10-45
Windows Media Transaction Logging	10-47
Log Formats Accepted by Windows Media Services 9	10-47
Windows Media Streaming Transaction Log Fields	10-48
Movie Streamer Transaction Log Fields	10-54
Flash Media Streaming Transaction Log Fields	10-56
Status Codes in Flash Media Streaming Access Logs	10-60
Events in Flash Media Streaming Access Logs	10-62
Service Router Transaction Log Fields	10-63
Where to Go Next	10-64

CHAPTER 11

Maintaining the Enterprise CDS 11-1

Upgrading Software	11-1
Obtaining the Upgrade	11-1
Pre-positioning the Upgrade Software File (optional)	11-2
Configuring the Software Image Settings	11-2
Upgrading the Software	11-5
Interoperability Considerations	11-6
Upgrading Software by Device Groups	11-7
Software Upgrades by Device	11-8
Finding the Device Software Version	11-9
Rebooting Devices	11-9
Individual Devices	11-9
Device Groups	11-9

Deleting a Device	11-10
Before Deleting a Device	11-10
Removing and Deregistering a Device Using CLI	11-11
Removing a Device with ECDSM	11-12
Deleting a Warm Standby ECDSM	11-13
Replacing a Device	11-13
Replacing a ECDSM	11-13
Replacing an SE or SR	11-14
Backup and Recovery	11-16
Performing Backup and Restore on the ECDSM Database	11-16
Recovering a Lost Administrator Password	11-17
Recovering ECDS Network Device Registration Information	11-18
Disk Maintenance	11-19
Disk Latent Sector Error Handling	11-19
Removing and Replacing Hard Disk Drives	11-20
Removing Content	11-21
Single Content Removal	11-21
Batch Content Removal	11-21
Where to Go Next	11-22

APPENDIX A

Troubleshooting A-1

Troubleshooting Tips for the CDSM	A-1
Troubleshooting Service Router Configurations	A-2
Verifying and Troubleshooting the Service Engine	A-3
Verifying and Troubleshooting WCCP	A-3
Show Commands	A-4
Show Command Examples	A-4
Debug Commands	A-6
Service Engine Debug Commands	A-6
Router Debug Commands	A-6
Debug Command Examples	A-6
GRE Packet Capture Commands	A-8
WCCP Logging	A-8
WCCP Logging Examples	A-8
Troubleshooting the Distribution Hierarchy	A-8
Determining the Distribution Path	A-9
Determining Reachability and Hierarchy	A-9
Troubleshooting Content Acquisition	A-10

[Enabling the Kernel Debugger](#) **A-13**

[Where to Go Next](#) **A-14**

APPENDIX B

Creating Manifest Files **B-1**

[Introduction](#) **B-1**

[Manifest File Requirements](#) **B-2**

[Working with Manifest Files](#) **B-2**

[Specifying a Single Content Item](#) **B-3**

[Specifying a Crawl Job](#) **B-4**

[Understanding the Prefix Attribute](#) **B-6**

[Writing Common Regular Expressions](#) **B-7**

[Scheduling Content Acquisition](#) **B-7**

[Specifying Shared Attributes](#) **B-7**

[Specifying a Crawler Filter](#) **B-8**

[Specifying Content Priority](#) **B-10**

[Generating a Playserver List](#) **B-11**

[Customized Manifest Playserver Tables and the HTTP Playserver](#) **B-11**

[Specifying Attributes for Content Serving](#) **B-12**

[Specifying Time Values in the Manifest File](#) **B-13**

[Refreshing and Removing Content](#) **B-13**

[Specifying Live Content](#) **B-14**

[Specifying Hybrid Ingest Content](#) **B-15**

[Manifest Validator Utility](#) **B-15**

[Running the Manifest Validator Utility](#) **B-16**

[Valid Manifest File Example](#) **B-16**

[Invalid Manifest File Example](#) **B-17**

[Understanding Manifest File Validator Output](#) **B-18**

[Syntax Errors](#) **B-19**

[Syntax Warnings](#) **B-19**

[Correcting Manifest File Syntax](#) **B-19**

[Manifest File Structure and Syntax](#) **B-19**

[Manifest File Tag Summary](#) **B-20**

[Manifest File Nested Tag Relationships](#) **B-22**

[Manifest File Tag Descriptions](#) **B-23**

[XML Schema](#) **B-46**

[Manifest XML Schema](#) **B-46**

[PlayServerTable XML Schema](#) **B-51**

[Default PlayServerTable Schema](#) **B-51**

[Manifest File Time Zone Tables](#) **B-52**

Standard Time Zones and GMT Offsets	B-52
GMT Offsets by Country	B-53
Africa	B-54
America	B-55
Antarctica/Arctic	B-56
Asia	B-56
Atlantic	B-57
Australia	B-57
Brazil	B-58
Canada/Chile/Cuba	B-58
Egypt/Europe	B-58
Hong Kong/Iceland/India/Iran/Israel	B-59
Jamaica/Japan/Kwajalein/Libya	B-59
Mexico/Mideast	B-60
Pacific/Poland/Portugal	B-60
Singapore/System V/Turkey	B-60
U.S.	B-61

APPENDIX C

Creating Coverage Zone Files C-1

Coverage Zone File Elements	C-1
Zero-IP Based Configuration	C-2
Coverage Zone XML Schema	C-3
Coverage Zone File Examples	C-6
Scenario 1: Coverage Zone with Client Network Only	C-6
Scenario 2: Coverage Zone with Geographical Location of the Datacenter Only	C-6
Scenario 3: Coverage Zone with Client Network and Geographical Location of the Datacenter	C-7
Scenario 4: Coverage Zone for Same Client Network with Different Weighted SEs	C-8

APPENDIX D

Creating Authorization Service Files D-1

Authorization Service Configuration File Elements	D-1
Authorization Service Configuration XML Schema	D-2
Authorization Service Configuration File Example	D-6

APPENDIX E

Verifying the Enterprise CDS E-1

Verifying the Web Engine	E-1
Verifying Preingested Web Content	E-1
Verifying Dynamically Ingested Web Content	E-3
Verifying the Windows Media Streaming Engine	E-7

Verifying Preingested Windows Media Content	E-7
Verifying Dynamically Ingested Windows Media Content	E-8
Verifying Windows Media Live Content Playback	E-10
Verifying the Movie Streamer Engine	E-11
Preparing Movie Streamer Content for Ingest	E-11
Verifying Preingested Movie Streamer Content	E-13
Verifying Dynamically Ingested Movie Streamer Content	E-16
Verifying Movie Streamer Live Content Playback	E-17
Verifying the Flash Media Streaming Engine	E-19
Verifying Flash Media Streaming Preingested Content	E-20
Verifying Flash Media Streaming Dynamically Ingested Content	E-22
Verifying Flash Media Streaming—Live Streaming	E-25

CHAPTER F

Configuring Primary and Backup Proxy Servers F-1

Configuring Primary Proxy Failover	F-2
Designating a Primary Outgoing HTTP Proxy Server	F-3
Designating a Primary Outgoing FTP Proxy Server	F-3
Designating a Primary Outgoing HTTPS Proxy Server	F-4
Configuring HTTP and HTTPS Outgoing Proxy Exclusion Settings	F-5
Monitoring Outgoing Proxy Servers and Statistics	F-7
Displaying the Current Outgoing Proxy Server Configuration	F-8
Displaying Outgoing Proxy Server Statistics	F-8

APPENDIX G

Software Licensing Information G-1

OpenSSL/Open SSL Project	G-1
License Issues	G-1
Open Source Used In Cisco Enterprise Content Delivery System 2.5.3	G-3

APPENDIX H

Unsupported Features H-1

Unsupported in Cisco ECDS	H-1
Unsupported in Cisco ECDS with WCCP	H-2
Where to Go Next	H-2



Preface



Tip

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Configuration Guide on Cisco.com.

The following sections describe:

- [What's in This Guide, page xvii](#)
- [Audience, page xvii](#)
- [Document Revision History, page xviii](#)
- [Document Organization, page xviii](#)
- [Document Conventions, page xx](#)
- [Related Documentation, page xxi](#)
- [Obtaining Documentation and Submitting a Service Request, page xxi](#)

What's in This Guide

This guide provides the information you need to configure and monitor the Cisco Enterprise Content Delivery System (Cisco ECDS). This guide does not describe system messages you might encounter or how to install your ECDS. See the [“Related Documentation” section on page xxi](#) for links to documentation online.

Audience

This guide is for the networking professional managing the Cisco ECDS. Before using this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of Ethernet, local area networking, and media streaming.

Document Revision History

Table 1 describes document update history. For complete support information, see the [Cisco ECDS 2.5 Release Notes](#).

Table 1 *Document Update History.*

Date	Notes
November 2010	Initial release.
September 2012	- Support for Cisco ECDS software up to Release 2.5.5 - WCCP and HTTPS protocol support in Release 2.5.5.

Document Organization

Table 2 describes the contents of this guide by chapter.

Table 2 *Document Organization*

Chapter or Appendix	Description
Chapter 1, “Product Overview”	Provides a brief introduction to the ECDS.
Chapter 2, “Network Design”	Describes the ECDS topology, elements of a delivery service, and the delivery service workflow.
Chapter 3, “Getting Started”	Provides information about initially configuring the devices to communicate with the Cisco Enterprise Content Delivery System Manager (CDSM), configuring a standby CDSM, navigating the CDSM, and a typical configuration workflow.
Chapter 4, “Configuring Devices”	Provides information about configuring the devices in the ECDS.
Chapter 5, “Configuring the Service Engine”	How to configure the Service Engine, including how to configure and manage features that require WCCP including IP Spoofing and HTTPS for application control Web settings.t.
Chapter 6, “Configuring the Service Router”	How to configure the Service Router.
Chapter 7, “Configuring WCCP”	How to configure WCCP and support features on your system.
Chapter 8, “Configuring Services”	Provides information about configuring delivery services.
Chapter 9, “Configuring the System”	Provides information on system configuration for the ECDS.
Chapter 10, “Monitoring the Enterprise CDS”	Provides information on monitoring the ECDS.

Table 2 **Document Organization**

Chapter or Appendix	Description
Chapter 11, “Maintaining the Enterprise CDS”	Provides information on upgrading the ECDS software, deleting devices from the system, performing disk maintenance, and removing content from the system.
Appendix A, “Troubleshooting”	Discusses troubleshooting Service Routers, and the acquisition and distribution of content.
Appendix B, “Creating Manifest Files”	Provides information on creating and validating a Manifest file.
Appendix C, “Creating Coverage Zone Files”	Provides information on creating and validating a Coverage Zone file.
Appendix D, “Creating Authorization Service Files”	Provides information on creating Authorization Service files.
Appendix E, “Verifying the Enterprise CDS”	Describes procedures for testing the ECDS using the different media players.
Appendix F, “Configuring Primary and Backup Proxy Servers”	How to configure primary and backup (failover) proxy servers.
Appendix G, “Software Licensing Information”	Provides information about the software licenses for the ECDS.
Appendix H, “Unsupported Features”	Provides information about features that may appear in the CDSM interface but which are not supported in the current release.

Document Conventions

Table 3 lists conventions for command syntax descriptions and textual emphasis:

Table 3 **Document Conventions**

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{x y z}	Alternative, mutually exclusive, keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <i>screen</i> font.
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen</i> font	Arguments for which you supply values are in <i>italic screen</i> font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets in contexts where italics are not available.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Caution

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



Note

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



Tip

Means the following information might help you solve a problem.

Related Documentation

For complete document support for the Cisco Media Delivery Engine appliances and the Cisco Enterprise Content Delivery System, see the *Documentation for the Enterprise Content Delivery System (ECDS)* document roadmap at the following link:

<http://www.cisco.com/en/US/docs/video/ecds/documentation.html>

Obtaining Documentation and Submitting a Service Request

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

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

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



CHAPTER 1

Product Overview

The following sections describe the Cisco Enterprise Content Delivery System (ECDS):

- [What is Cisco ECDS, page 1-1](#)
- [How Cisco ECDS Works, page 1-3](#)
- [Content Delivery System Architecture, page 1-6](#)
- [Where to Go Next, page 1-33](#)

What is Cisco ECDS

The Cisco ECDS is a distributed network of Media Delivery Engines (MDEs) running Content Delivery Applications (CDAs) that collaborate with each other to deliver multi-format content to a variety of client devices. The client devices supported are personal computers and Wi-Fi-enabled mobile devices, such as personal digital assistants (PDAs).

The ECDS supports a variety of mechanisms to accelerate the distribution of content within the content delivery network. The ECDS offers an end-to-end solution for enterprises to ingest and stream video to viewers throughout the enterprise.

The ECDS functionality can be separated into four areas:

- Ingest
- Distribution
- Delivery
- Management

Each MDE in the ECDS contributes to one or more of these functions as determined by the CDAs running on it. [Table 1-1](#) describes the relationship between the CDA names and the Cisco Enterprise Content Delivery System Manager (CDSM) device names.

Table 1-1 CDA Mapping to Functionality and CDSM

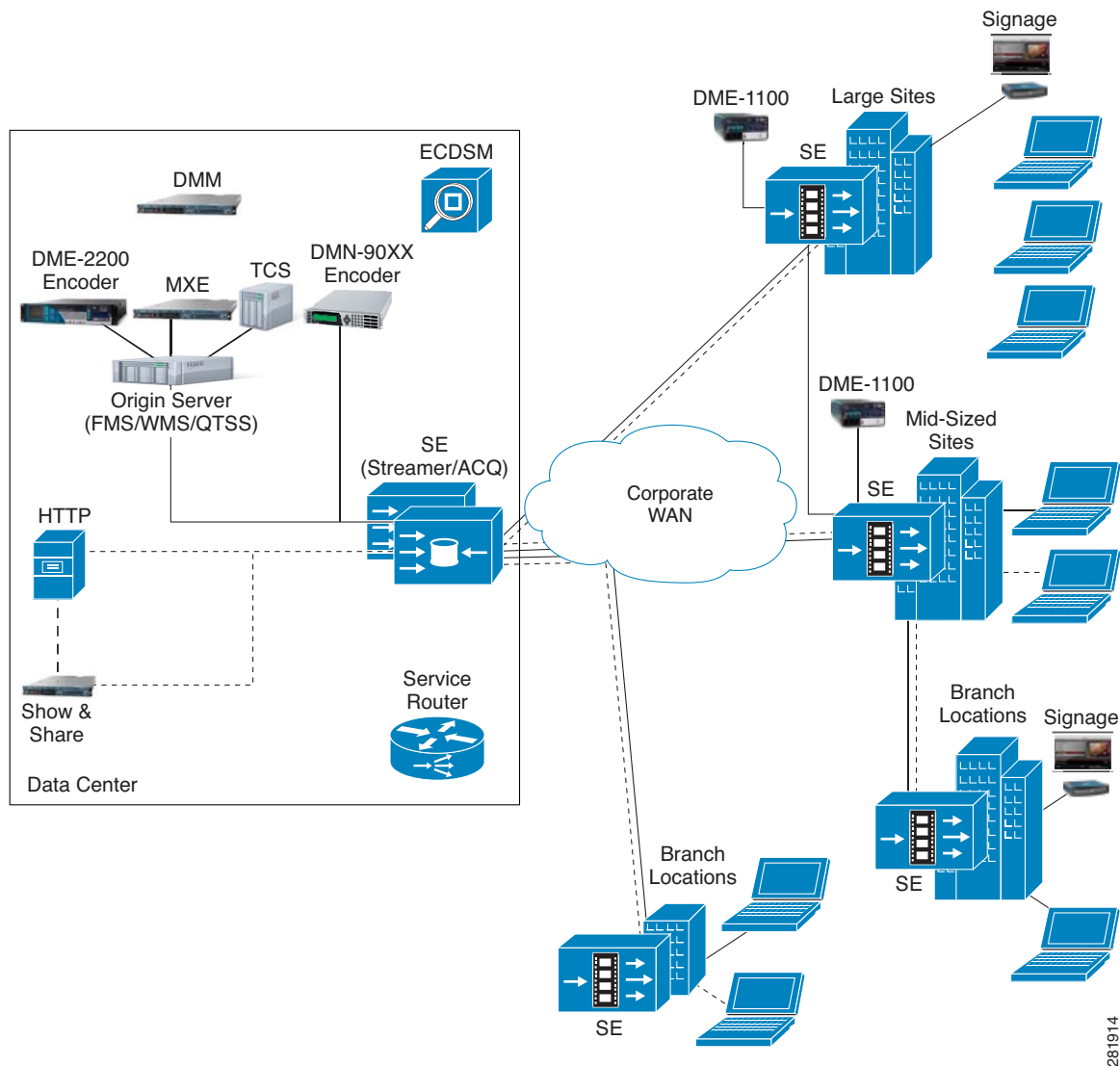
CDA Name	Functionality	CDSM Device Name
Media Streamer (+ Content Acquirer)	Ingest, distribution, and delivery	Service Engine (SE)
Service Router	Redirect client requests for delivery	Service Router (SR)
Enterprise Content Delivery System Manager	Management	CDSM

The Service Engine can function as a Content Acquirer (CA) and Media Streamer, or just as a Media Streamer.

Figure 1-1 shows the major elements of an ECDS network. How content flows, from ingest to distribution within the ECDS, to delivery to client devices, is dictated by the content delivery services defined for each Content Origin. A delivery service is a configuration defined by using the CDSM and consists of configuration parameters that dictate how content is ingested and distributed, and what content is delivered to the client devices. Some of the primary delivery service definition parameters include:

- Origin server
- Service routing domain name
- Service Engines participating in the delivery service
- Service Engine designated as the Content Acquirer

The Content Acquirer is only active on one Service Engine in each delivery service.

Figure 1-1 High-Level View of the Cisco ECDS

How Cisco ECDS Works

The following sections briefly describe the elements of the ECDS:

- [Ingest and Distribution, page 1-4](#)
- [Delivery, page 1-5](#)
- [Management, page 1-6](#)

For more detailed information, see the “[Content Delivery System Architecture](#)” section on page 1-6.

Ingest and Distribution

The Service Engine designated as the Content Acquirer for a delivery service is the ingest device. Cisco ECDS supports the following methods of content ingest:

- [Prefetch Ingest, page 1-4](#)
- [Dynamic Ingest, page 1-4](#)
- [Hybrid Ingest, page 1-5](#)
- [Live Stream Ingest and Split, page 1-5](#)

The distribution of content within the ECDS is determined by the method of ingest used.

**Note**

The maximum supported number of prefetched content items is 200,000.

Prefetch Ingest

The Content Acquirer receives metadata from the backoffice in the form of an XML-formatted Manifest file, which pulls the content into storage on the Content Acquirer using the information in the Manifest file. The content can be ingested by using the following supported protocols:

- HTTP
- HTTPS
- CIFS
- Local files, which are files copied to the Service Engine

The ingested content is then distributed to all Service Engines in the content delivery service. The content is stored on each Service Engine's hard disk for a configurable amount of time or until the content entry gets deleted from the Manifest file. This is called *content pinning*.

The Manifest file can be used to specify different policies for content ingest and also for streaming the prefetched content. For example, the policy could include specifying the expiry of the content, setting time windows in which the content is made available to users, and so on.

**Note**

The maximum supported number of content files that can be prefetched on each SE is 200,000.

Dynamic Ingest

Content can be dynamically ingested into the ECDS. Dynamic ingest is triggered when a Service Engine's Media Streamer application does not find a client's requested content in its local hard disk storage. All Service Engines participating in the content delivery service coordinate to form a content distribution tunnel starting at the origin server and ending at the Service Engine responding to the client request. As the content flows through this tunnel, the participating Service Engines cache a copy of the content. Subsequent requests for the same content are served off the ECDS network. Content ingested and distributed by this method is deleted if clients do not request it frequently.

The Cisco CDSM manages this ingest method internally, not by instructions embedded in a Manifest file, and manages the storage automatically. The Cisco CDSM also provides the ability to purge any dynamically ingested content out of the Service Engines. Content is identified by a URL, which is also used to delete the content.

Hybrid Ingest

The hybrid ingest method provides a very powerful solution by combining the features of the prefetch ingest and the dynamic ingest methods. The metadata and control information about the content, defined in the Manifest file, is propagated and pinned to all Service Engines participating in the content delivery service. However, the content is not prefetched. Ingest occurs upon user request for the content. Content that is cached on the Service Engines by using this method is subject to the same deletion rules as the dynamic ingest method. The metadata that is propagated can be used to specify explicit controls and policies for streaming the content.

**Note**

In the current release, the origin server OFQDN is always used, and the hostname/port in the Manifest file is ignored.

See the following sections for more information:

- [“Content Acquirer Selection for Dynamic or Hybrid Ingest” section on page 2-5](#)
- [“Specifying Hybrid Ingest Content” section on page B-15](#)

Live Stream Ingest and Split

The live stream ingest method distributes a live content feed to all the Service Engines participating in the content delivery service and helps to scale the content delivery to a very large audience. This method leverages the live stream splitting capabilities of the Media Streamer application and optimizes the access by doing a one-to-many split to all Service Engines in the content delivery service. The Cisco EDSM provides the necessary interface to schedule the streaming of live programs. Advanced techniques are used to enhance the performance of live streaming.

Delivery

The Service Router handles client requests for content and determines the best Service Engine to deliver it based on proximity, load, and health states.

Once the best Service Engine has been determined, the content is delivered to the client device by means of one of the following mechanisms:

- **Static Content Download Using HTTP**—Content is downloaded by the client device before it can be rendered to the user.
- **Progressive Content Download Using HTTP**—Content is rendered in segments to the user before it has been fully downloaded.
- **Content Streaming Using HTTP, RTMP, RTSP, or RTP**—Content is streamed to the client device, Service Engines collect feedback and can fine-tune streaming. Advanced error recovery can also be performed. This is a very common method of streaming video content to client devices. Real-Time Messaging Protocol (RTMP) is part of the Flash Media Streaming feature. RTMP support is for managed domains only.

Request Routing

ECDS supports two types of routing:

- **Routing Using WCCP**—In the WCCP transparent routing method, requests for content made to an origin server are intercepted by a WCCP-enabled router. The WCCP-enabled router transparently redirects the request to a Service Engine. This type of transparent redirection allows traffic interception on any traffic port on a specific router. WCCP contains many fail-safe mechanisms to ensure that the request interception remains entirely transparent to the end user. See the [“Routing Using WCCP” section on page 1-28](#) for more information.
- **Routing Using the Service Router**—The *Service Router* mediates requests from the client devices and redirects the requests to the most appropriate Service Engine. It monitors the load of the devices and does automatic load balancing.

The Service Router is the authoritative Domain Name System (DNS) server for the routed request for the fully qualified domain name (FQDN) of the origin server. In other words, the Request Routing Engine responds to any DNS queries for that domain.

This type of Request Routing uses RFQDN-based redirection. See the [“RFQDN Redirection” section on page 1-21](#) for more information.

Management

The Enterprise CDSM, a secure Web browser-based user interface, is a centralized system management device that allows an administrator to manage and monitor the entire ECDS network. All devices, Service Engines and Service Routers, in the ECDS are registered to the Enterprise CDSM.

Service Engines can be organized into user-defined device groups to allow administrators to apply configuration changes and perform other group operations on multiple devices simultaneously. One device may belong to multiple device groups.

The Enterprise CDSM also provides an automated workflow to apply a software image upgrade to a device group.

Content Delivery System Architecture

The ECDS consists of an Enterprise CDSM, one or more Service Engines, and one Service Router. For full redundancy, an ECDS would include an additional CDSM and Service Router. The Service Engine handles content ingest, content distribution within the ECDS, and content delivery to client devices. The Service Router handles client requests and redirects the client to the most appropriate Service Engine. The Enterprise CDSM manages and monitors the ECDS, the delivery services, and all the devices in the ECDS.

This section describes the following:

- [Service Engine](#)
- [Service Router](#)
- [Content Delivery System Manager](#)
- [Resiliency and Redundancy](#)

Service Engine

Each Service Engine can function both as a [Content Acquirer](#) and [Media Streamer](#), or just as a Media Streamer. Based on the Service Engines' assignments to different delivery services, the right set of applications supporting the functions is enabled. For example, only one Service Engine is assigned the role of Content Acquirer in each delivery service. In addition, the Service Engine assigned as the Content Acquirer in a delivery service also includes the functions of an Media Streamer.

Both the Content Acquirer and the Media Streamer applications have storage and distribution functions within the ECDS, which include the following:

- Management of content and metadata physical storage. Content URLs are translated into their physical file paths for content retrieval, deletion, and update.
- Management of dynamically ingested content and periodic replacement of content not frequently accessed. Content replacement is performed by sophisticated content-replacement algorithms. The algorithms add “*weight*” to the content according to size, frequency of access, and other attributes to produce the list of content that needs to be purged.
- Ingest of prefetched content and retrieval of such content for distribution to other Service Engines in the same delivery service.
- Maintenance of information about the entire ECDS topology and all the delivery services. This includes upkeep of a list of Service Engines in the same delivery service that is used for distributing prefetched, dynamic, and live stream content.
- Maintenance of the database that stores and distributes metadata about the content, and the topology and delivery service information.
- Distribution of content on a per-delivery service basis, where the flow path of content could differ from one delivery service to another.

See the following sections for more information:

- [Content Acquirer, page 1-7](#)
- [Media Streamer, page 1-8](#)

Content Acquirer

Every delivery service requires a Content Acquirer, which is a CDA that resides on every Service Engine. The Content Acquirer CDA becomes active when the Service Engine is designated as the Content Acquirer in a delivery service. The Content Acquirer has the following functions and capabilities:

- Fetches content from origin servers using HTTP, HTTPS, or CIFS (Dynamic ingest supports HTTP only).
- Supports the NT LAN Manager (NTLM) and basic authentication for ingesting content from the origin servers.
- Creates and distributes the metadata for each of the prefetched contents according to the Manifest file and the information returned by the origin server.

Once the Content Acquirer has ingested the content and distributed the metadata, it creates a database record for the metadata and marks the content ready for distribution. All other types of ingest (dynamic, hybrid, and live stream) are handled by the Content Acquirer as well.

Media Streamer

All Media Streamers participating in a delivery service pull the metadata from a peer Media Streamer called a *forwarder*, which is selected by the internal routing module. Each Media Streamer participating in a delivery service has a forwarder Media Streamer. The Content Acquirer is the top-most forwarder in the distribution hierarchy. In the case of prefetched ingest, each Media Streamer in the delivery service looks up the metadata record and fetches the content from its forwarder. For live or cached content metadata, only the metadata is distributed.

The content associated with the metadata for live and cached content is fetched by the specified protocol engine, which uses the dynamic ingest mechanism. When a request for a non-prefetched content arrives at a Media Streamer, the protocol engine application gets the information about the set of upstream Media Streamers through which the content can be acquired. In the case of dynamic ingest, the Media Streamer uses the cache routing function to organize itself as a hierarchy of caching proxies and performs a native protocol cache fill. Live stream splitting is used to organize the Media Streamers into a live streaming hierarchy to split a single incoming live stream to multiple clients. The live stream can originate from external servers or from ingested content. Live stream splitting is supported on the following:

- Windows Media Engine
- Movie Streamer Engine
- Flash Media Streaming Engine

The Media Streamers use service control to filter and control incoming requests for content. The service rules are encapsulated under the Service Control option in the Enterprise CDSM.

The Media Streamers send keep-alive and load information to the Service Router that is participating in the same delivery service. This information is used by the Service Router to choose the most appropriate Media Streamer to handle the request.

The Media Streamer function is implemented as a set of protocol engine applications. The protocol engine applications include the following:

- [Web Engine](#)
- [Windows Media Engine](#)
- [Movie Streamer Engine](#)
- [Flash Media Streaming Engine](#)

Web Engine

All HTTP(S) client requests that are redirected to a Service Engine by the Service Router are handled by the Web Engine. On receiving the request, the Web Engine uses its best judgment and either handles the request or forwards it to another component within the Service Engine. The Web Engine, using HTTP(S), can serve the request from locally stored content in the ECDS or from any upstream proxy or origin server.

An HTTP(S) client request that reaches the Service Engine can either be from a Service Router redirect or from a direct proxy request.

On receiving an HTTP(S) request for content, the Web Engine decides whether the content needs to be streamed by the Windows Media Engine, and if so, hands the request over to the Windows Media Engine, otherwise the request is handled by the Web Engine.

For more information, see the following sections:

- [Cache-Fill Operations, page 1-9](#)

- [Authentication, page 1-10](#)
- [Service Rules, page 1-10](#)

Cache-Fill Operations

The Web Engine interfaces with the storage function in the Service Engine to determine whether the content is present locally or whether the content needs to be fetched from either an upstream Service Engine or the origin server.

The Web Engine communicates to the upstream Service Engine for cache-fill operations. This interaction is based on HTTP(S). This cache-fill operation is on demand and hence only occurs when the content is not stored locally. The upstream Service Engine can be selected dynamically by means of the Hierarchical Cache Routing Module, or can be configured statically through the Enterprise CDSM. The Hierarchical Cache Router generates a list of upstream Service Engines that are alive, ready to serve the request, and part of the delivery service. If the Web Engine is unsuccessful in locating the content on one of these Service Engines, the content is retrieved from the origin server.

Whether the content is found locally or retrieved and stored through the cache-fill operation, the Web Engine serves the content based on the following:

- **Freshness of content**—The freshness of prefetched content is governed by a time-to-live (TTL) value set for the content in the delivery service configuration. The TTL specifies the rate at which content freshness is checked. This setting is configured for each delivery service either by using the CDSM or by specifying this setting in the Manifest file for the delivery service.

For cached content, which is content ingested by means of the dynamic ingest or the hybrid ingest method, the freshness check is performed by the Web Engine in compliance with RFC 2616. If the origin server does not provide an expiry time, the Web Engine uses the age multiplier setting, the minimum TTL setting, and the maximum TTL setting to determine the freshness of the content.



Note

This algorithm is used to determine freshness for cached content based on the expire time. It is not used to determine the popularity of the content.

This expiry header validation is just one case to decide whether content revalidation is needed or not. Revalidation is also decided based on cache control headers that are part of request headers, and the min-fresh, max-stale, max-age parameters that can come in both request and response headers.

If the origin server provides the expire time, it is used to determine the freshness of the content. If the expire time is not available, the expire time of the content is calculated as follows:

$\text{Expire\_time} = (\text{Create\_time} - \text{Last\_modified\_time\_from\_origin\_server}) * \text{age multiplier}$

The *create time* is the time on the ECDS when the content was cached. The *last modified time* is the time the content was last modified on the origin server. The age multiplier value (as a percentage) is used to shorten the time it takes to have the content revalidated.

For example, if the create time was May 5, 2009 12:00 and the origin server last modified the content on May 1, 2009 12:00, then the expire time would be 4 days. If the age multiplier was set to 50 percent, the expire time would be 2 days.

The calculated expire time is compared with the minimum TTL and maximum TTL settings. If the expire time is greater than the maximum TTL, the maximum TTL is used as the expire time. If the expire time is less than the minimum TTL, the minimum TTL is used as the expire time.

Using the example above, if the minimum TTL was 3 days and the calculated expire time was 2 days, then the minimum TTL is used as the expire time. If the maximum TTL is 10 days, then the calculated expire time still uses the minimum TTL of 3 days as the expire time. The min/max TTL algorithm follows:

Expire_time = if (MINTTL < Expire_time < MAXTTL), then Expire_time
 else if Expire_time < MINTTL, then MINTTL
 else MAXTTL

The expire time is compared with the *cache age* in order to determine whether the content needs to be revalidated by the origin server. If the cache age is less than or equal to the expire time, then the content is considered fresh. The following calculation is used to determine the cache age:

Cache_age = Current_time – Create_time

In our example, if the current time is May 25, 2009 12:00 and the create time is May 5, 2009 12:00, then the cache age is 20 days. The cache age of 20 days is compared to the expire time, which in our example is 2 days, and because the cache age is greater than the expire time the content is revalidated with the origin server. When the content is revalidated it gets a new create time. To compute a more accurate cache age, the response delay is considered. The *response delay* is calculated as follows:

Response_delay = Create_time – Time_request_sent_to_origin_server

In our example, the create time is May 5, 2009 12:00, and if the origin server takes 2 minutes to respond to the request for content (because of network-imposed delays), the response delay is May 5, 2009 11:58. This allows the cache age to be calculated based on the time the request was initiated, not the time the response was received.

- **Rate of data transfer**—The rate at which the content is sent can be configured on a per-delivery basis. By default, LAN bandwidth is used.
- **Content completeness**—Prefetched content is stored locally in the ECDS in its entirety. For cached content, there are two cases when the content is not complete:
 - The Web Engine process halts or the Service Engine experiences a failure in the process of caching the content. In this case, the subsequent request starts the cache fill anew.
 - The content is in the process of being cached by another request. In this case, the subsequent request is served from the cached content.

Authentication

The Web Engine supports a pass-through mode of authentication, whereby the origin server negotiates authentication and the Web Engine passes the requests and responses between the client device and the origin server. Content that requires authentication is not cached by the Service Engine, so all requests for authenticated content are retrieved from the origin server.

Service Rules

Service rules can be configured that dictate how the Web Engine responds when client requests match specific patterns. The patterns can be a domain or host name, certain header information, the request source IP address, or a Uniform Resource Identifier (URI). Some of the possible responding actions are to allow or block the request, or rewrite or redirect the URL.

Windows Media Engine

The Windows Media Engine uses Windows Media Technology (WMT), a set of streaming solutions for creating, distributing, and playing back digital media files across the Internet. WMT includes the following applications:

- Windows Media Player—End-user application
- Windows Media Server—Server and distribution application
- Windows Media Encoder—Encodes media files for distribution
- Windows Media Codec—Compression algorithm applied to live and on-demand content
- Windows Media Rights Manager (WMRM)—Encrypts content and manages user privileges

The Windows Media Engine streams Windows Media content, with the capability of acting both as a server and as a proxy. It streams prefetched content to the Windows Media Player, acts as a proxy for client requests, splits a live stream into multiple live streams, and caches content requested from remote servers.

Windows Media Engine acts as Windows Media Server for prefetched or cached content stored locally. The request is served by RTSP and HTTP. Windows Media Engine checks with the storage function on the Service Engine to see whether the content is stored locally; if the content is not found, the Windows Media Engine engages the Windows Media Proxy.

The WMT Proxy works like the cache-fill operation in the Web Engine. See the [“Cache-Fill Operations” section on page 1-9](#). There are two options:

- Hierarchical Caching Proxy—If content is not found locally, the Windows Media Engine checks the upstream Service Engines first before pulling the content from the origin server.
- Static Caching Proxy—The administrator statically configures Service Engines as upstream proxies.

The WMT Proxy accepts and serves streaming requests over RTSP and HTTP.

For more information, see the following sections:

- [Fast Start, page 1-11](#)
- [Fast Cache, page 1-11](#)
- [Fast Stream Start, page 1-12](#)
- [Live Stream Splitting, page 1-12](#)
- [Authentication, page 1-13](#)
- [Bandwidth Management, page 1-13](#)
- [Policy Server Integration, page 1-14](#)

Fast Start

Fast Start provides data directly to the Windows Media Player buffer at speeds higher than the bit rate of the requested content. After the buffer is filled, prefetched, cached, or live content stream at the bit rate defined by the content stream format. Fast Start does not apply to content that is dynamically ingested. Only Windows Media 9 Players that connect to unicast streams using MMS-over-HTTP or RTSP can use Fast Start. The Fast Start feature is used only by clients that connect to a unicast stream. With live content, the Windows Media Engine needs to hold the content in its buffer for a few seconds. This buffer is used to serve Fast Start packets to subsequent clients that request the same stream as the initiating first client request. The first client triggers the process, with the subsequent clients benefitting from Fast Start.

Fast Cache

Fast Cache allows clients to buffer a much larger portion of the content before rendering it. Fast Cache is supported only for TCP. The Windows Media Engine streams content at a much higher data rate than specified by the stream format. For example, using Fast Cache, the Windows Media Engine can transmit a 128-kilobit per second (Kbps) stream at 700 Kbps. This allows the client to handle variable network

conditions without perceptible impact on playback quality. Only MMS-over-HTTP and RTSP requests for prefetched or cached content support Fast Cache. The speed is determined by the client's maximum rate and the configured Fast Cache rate—whichever is smaller.

Fast Stream Start

The first client requesting a live stream often experiences the longest wait time for the content to begin playing. Users can experience long wait times because of the full RTSP or HTTP negotiation that is required to pull the live stream from the source. Delays can also occur if the edge Service Engine has not buffered enough stream data to fill the player's buffer at the time the content is requested. When the buffer is not filled, some data to the client might be sent at the linear stream rate, rather than at the Fast Start rate. With Fast Stream Start, when a live stream is primed, or scheduled and pulled, a live unicast-out stream is pulled from the origin server to a Service Engine before a client ever requests the stream. When the first request for the stream goes out, the stream is already in the delivery service.

Live Stream Splitting

Live stream splitting is a process whereby a single live stream from the origin server is split and shared across multiple streams, each serving a client that requested the stream. When the first client that requested the stream disconnects, the Windows Media Engine continues to serve the subsequent requesting clients until all requesting clients have disconnected. Live stream splitting using content that is already stored locally is generally better than using content from the origin server; this is because the Service Engine is typically closer to the requesting clients, and therefore network bandwidth to the origin server is freed up.

**Note**

When using Windows Media Server 2008 as the origin server, the source content type must be a playlist or encoder type.

Live stream splitting can either be unicast or multicast, depending on the configuration, capabilities and limitations of the network. The Windows Media Engine can receive and deliver Windows Media content over IP multicast or unicast transmission in the following combinations:

- Multicast-Out
- Unicast-Out
- Unicast-In Unicast-Out
- Multicast-In Unicast-Out

**Note**

For multicast-in (to the SE) to work, the network needs to be multicast-enabled.

Multicast-Out

The Windows Media Engine can be used in a live or rebroadcast program to deliver multicast streams to client devices. The source of the stream can be multicast, unicast, or a local file. The program can be scheduled, continuous, or play once. The content can be either live or rebroadcast. The Windows Media Engine creates a Windows Media file (.nsc) that contains session information including the multicast IP address, port, time-to-live (TTL), and so on. The client requests the .nsc file using HTTP. Once the file is downloaded, the client parses it and sends an Internet Group Management Protocol (IGMP) join to receive the multicast stream. A client can start and stop the stream, but cannot pause, fast-forward, or rewind it.

Unicast-Out

The Windows Media Engine can act as a broadcast publishing point to deliver live streams, prefetched/cached content, or content from dynamic ingest, to a requesting client. The source of the stream can be multicast, unicast, or a local file. The Windows Media Engine can also perform live stream splitting if more than one client requests the same content. The delivery service can be used to simulate an experience similar to viewing a TV program even if the source of the stream is a Video On Demand (VOD) file. A client can start and stop the stream but cannot pause, fast-forward, or rewind it. When a delivery service is configured, a client makes a request to the Windows Media Engine, which is acting as the Windows Media Server, and the Windows Media Engine checks to see whether the incoming stream is present. If it is, the Windows Media Engine joins the stream and splits it to the new client. If the request is the first client request for this stream, the Windows Media Engine sends the request to the origin server and then serves it to the new client.

Authentication

The Windows Media Engine supports pass-through authentication. The following authentication mechanisms are supported in pass-through mode:

- Anonymous
- NTLM
- Negotiate (Kerberos)
- Digest access authentication

With pass-through authentication, the Windows Media Engine establishes a tunnel between the client and the origin server so that the origin server can authenticate the client.

Bandwidth Management

Bandwidth management of Windows Media content can be controlled by setting limits for incoming and outgoing bandwidth and session bit rate and Fast Start maximum bandwidth. In addition, in the case of live streaming, contributing origin servers can be identified to allow incoming content to exceed the bandwidth check to support high demand scenarios. The Windows Media bandwidth management capabilities are described in [Table 1-2](#).



Tip

We recommend that customers with variable bit rates cap the bit rate at the encoder to avoid bit rate spikes, which may result in throughput exceeding the supported throughput allowed in the Cisco ECDS. Use the **show bitrate [movie-streamer | wmt]** command in EXEC configuration mode to display the bit rate allocated to a particular device. Use the **bitrate** command in Global configuration mode to configure the maximum pacing bit rate for large files for the Movie Streamer and to separately configure WMT bit-rate settings.

Table 1-2 **Bandwidth Management Capabilities**

Bandwidth Management	Description
Incoming Bandwidth	The bandwidth for Windows Media content coming into the Service Engine, from either an upstream Service Engine or from the origin server.
Outgoing Bandwidth	The bandwidth for streaming Windows Media content to the end user from the Service Engine.
Incoming Session Bit Rate	The maximum bit rate per session that can be delivered to the Service Engine from the origin server or upstream Service Engine.

Table 1-2 Bandwidth Management Capabilities (continued)

Bandwidth Management	Description
Outgoing Session Bit Rate	The maximum bit rate per session that can be delivered to a client.
Incoming Bandwidth Bypass List	The list of identified hosts allowed to bypass the incoming bandwidth check for broadcast or multicast live content.
Fast Start Maximum Bandwidth	Maximum bandwidth allowed per player when Fast Start is used to serve packets to each player. Increased bandwidth initially used by the Fast Start feature can overburden a network if many players connect to the stream at the same time. To reduce the risk of network congestion caused by the Fast Start feature, limit the amount of bandwidth the Fast Start feature uses to stream to each player.

Policy Server Integration

The Windows Media Engine uses HTTP and RTSP to send start, stop, and pause messages to the policy server.

Movie Streamer Engine

The Movie Streamer Engine is an open-source, standards-based, streaming server that delivers hinted MPEG-4, hinted 3GP, and hinted MOV files to clients over the Internet and mobile networks using the industry-standard RTP and RTSP. Hinted files contain hint tracks, which store packetization information that tell the streaming server how to package content for streaming.

The Movie Streamer Engine is an RTSP streaming engine that supports Third Generation Partnership Project (3GPP) streaming files (.3gp). Support of 3GPP provides for the rich multimedia content over broadband mobile networks to multimedia-enabled cellular phones.

**Note**

The streaming capability of Movie Streamer Engine only depends on the movie file format or stream transport type. It is independent of codec types. Movie Streamer supports any client player that can fetch media streams by way of RTSP or RTP. However, the client player must have the correct codec in order to render the stream correctly.

The Movie Streamer Engine can act as both a server and a proxy. It streams prefetched or RTSP-cached content to RTSP clients, acts as a proxy for client requests, splits a live stream into multiple live streams, and caches content requested from remote servers.

After the RTSP request comes into the Movie Streamer, the URI in the RTSP request is modified to reflect the result of the mobile capability exchange. The Movie Streamer checks with the storage function on the Service Engine to see whether the content is stored locally. If the content is not found or if an RTSP-cached content version needs freshness validation, the Movie Streamer engages the Movie Streamer proxy.

In the case of an RTSP-cached content version verification, the Movie Streamer proxy forwards the DESCRIBE request to the origin server for a response containing the Last-Modified-Time header in the response. If the Last-Modified-Time matches the cached version, the Movie Streamer streams the cached content; otherwise, the Movie Streamer proxy forwards the request to the origin server for RTSP negotiation. A client session and a server session are created with the following attributes:

- Server session is responsible for connecting to the origin server to fetch the content and cache it locally. The server session generates the media cache file and the linear hint files.
- Client session is responsible for streaming the locally cached file to the client.
- Client and server sessions are separated so that multiple server sessions can be spawned for the same URL to cache content from different starting points or at faster speeds, or both. This increases the speed of fetching the content. The client session starts to stream from the cached content that the server session is writing.

The Movie Streamer proxy works like the cache-fill operation in the Web Engine and the Windows Media Engine, except for the minimum TTL value. The Movie Streamer's minimum TTL value is always zero. See the [“Cache-Fill Operations” section on page 1-9](#). There are two options:

- **Hierarchical Caching Proxy**—If content is not found locally, the Movie Streamer checks the upstream Service Engines first before pulling the content from origin server.
- **Static Caching Proxy**—The administrator statically configures Service Engines as upstream proxies.

The Movie Streamer supports basic pass-through proxy mode for certain conditions where caching cannot be performed. Such conditions include, but are not limited to, the Service Engine running out of disk space.

For more information, see the following sections:

- [Transport Types, page 1-15](#)
- [Live Stream, page 1-15](#)

Transport Types

Prefetched content can be delivered by the non-accelerated method or the accelerated method.

Non-prefetched content (proxied or cached content) is always delivered by the accelerated method. The content is delivered to the client device by one of the following mechanisms:

- **Non-Accelerated**—This method has limited concurrent streams and total throughput, but supports many transport formats. The non-accelerated method supports the following transport formats:
 - RTP over UDP
 - Reliable UDP
- **Accelerated**—This method supports only RTP over UDP. Content must be reprocessed by the Movie Streamer Linear Hiner. The linear hiner process can be initiated manually by the administrator or dynamically triggered by the first request for the content.

The Movie Streamer Linear Hiner process may take a while, so the first request that triggers this process is served by the non-accelerated method. All subsequent requests are served by the accelerated method.

The first client request for content that requires proxying or caching experiences a delay, because all proxying and caching requires the accelerated method.

Live Stream

The Movie Streamer Engine supports multicast reference URLs (Announce URLs) for programs that are created through the Enterprise CDSM. The multicast reference URL, which is in the form of `http://Service Engine IP address/Program ID.sdp`, is resolved by the Movie Streamers that are serving the live program.

QuickTime live typically has a UDP socket pair (for RTP and RTCP) per track, and each client session typically has two tracks (audio and video).

**Note**

The following rules apply to live splitting:

1. For unicast streaming, the client request must be sent by RTSP.
2. For multicast streaming, the client request must be sent by HTTP.

Flash Media Streaming Engine

The Flash Media Streaming Engine incorporates the Adobe Flash Media Server technology into the ECDS platform. The Flash Media Streaming Engine is capable of hosting Flash Media Server applications that are developed using ActionScripts, such as VOD (prefetched content, or dynamic or hybrid ingested content), live streaming, and interactive applications.

**Note**

The Cisco ECDS Flash Media Streaming Engine supports the Adobe Flash Media Rights Management Server (FMRMS) for VOD content; it is not supported for live streaming. Adobe FMRMS protects media content delivered to Adobe Media Player and Adobe AIR applications. FMRMS is also available for proxied content, if Adobe supports the content type. For more information about the Adobe Flash Media Rights Management Server, see www.adobe.com.

**Note**

ECDS supports the Adobe Flash Media Server Administration application programming interfaces (APIs) and the Administration Console that was built using the Administration APIs. These APIs can be used to monitor and manage the Adobe Flash Media Server running on a Cisco ECDS Service Engine. See the “[Configuring Flash Media Streaming](#)” section on page 5-37 for more information.

Upon receiving a client request for VOD content, the edge Service Engine does the following:

- If the content is present, the edge Service Engine streams it using RTMP.
- If the content is not present, the edge Service Engine uses HTTP to fetch the content from the origin server and serves it using RTMP.

No client information is sent to the origin server. No per-client control connection is present between the edge Service Engine and the origin server for VOD streaming.

HTTP Requests

Flash Media Streaming encompasses all flash applications, from simple Flash Video (FLV) files to more complex Small Web Format (SWF) files. All HTTP client requests for SWF files, that are redirected to a Service Engine by the Service Router, are handled by the Web Engine. The Web Engine, using HTTP, serves the request from locally stored content in the ECDS or from any upstream Service Engine or origin server. See the “[Web Engine](#)” section on page 1-8 for more information.

RTMP Requests

The SWF file is a compiled application that runs on the Adobe Flash Player, and may contain RTMP calls to FLV, MPEG-4 (H.264), or MP3 files. RTMP calls, in the form of URL requests, are routed to a Service Engine by the Service Router.

Flash Media Streaming supports RTMP and RTMPE on port 1935 only. RTMPE is the secure flash streaming technology from Adobe. Encrypted RTMP (RTMPE) is enabled on Flash Media Streaming by default, and allows you to send streams over an encrypted connection without requiring certificate management.

**Note**

The Service Router uses RTMP redirection to direct the client's Flash Player to the best Service Engine based on load balancing and resiliency. RTMP redirections are supported only by Adobe Flash Player 9. All older Flash Players do not support RTMP redirection.

**Note**

For VOD streams, all RTMP calls in the SWF file must be in the following format:

```
rtmp://rfqdn/vod-ecds/path/foo.flv
```

In this format, *rfqdn* is the routing domain name of the Service Router, *vod-ecds* is the required directory, and *path* is the directory path to the content file that conforms to the standard URL specification.

If you are unable to store the VOD content in the required *vod-ecds* directory on your origin server, you can create a VOD virtual path for all RTMP requests. All client requests for RTMP calls still use the `rtmp://rfqdn/vod-ecds/path/foo.flv` format for VOD streams, but the SE replaces the *vod-ecds* directory with the string specified in the **flash-media-streaming application-virtual-path vod-ecds map** command.

Use the **flash-media-streaming application-virtual-path vod-ecds map <mapping string>** command on each SE participating in a Flash Media Streaming delivery service. The mapping string variable accepts all alphanumeric characters and the slash (/) character, and can be from 1 to 128 characters. For example, to map the "vod-ecds" directory to "media" for the go-tv-stream.com origin server, use the **flash-media-streaming application-virtual-path vod-ecds map media** command.

Use the **flash-media-streaming application name live-ecds** for Live flash-media-streaming delivery services.

If comedy.flv is the content being requested, the RTMP call in the SWF file would be `rtmp://go-tv-stream.com/vod/comedy.flv`. The SE would replace the "vod" directory and request `http://go-tv-stream.com/media/comedy.flv` from the upstream SE or origin server.

If just the slash (/) character is used to replace the "vod-ecds" directory, the SE request would be `http://go-tv-stream.com/comedy.flv`.

For prefetched and cached content, the Flash Media Streaming Engine uses RTMP or RTMPE over port 1935. For content that is not found locally, the Flash Media Streaming Engine communicates with the Web Engine, that in turn communicates with the upstream Service Engine for cache-fill operations. See the ["Cache-Fill Operations" section on page 1-9](#). This interaction uses HTTP. Once the content is in the process of being retrieved by the Web Engine, the Flash Media Streaming Engine uses RTMP to begin streaming the content.

The following describes the characteristics of caching content using HTTP for RTMP client requests:

1. Origin server-based cache validation is still honored for the cached content.
2. Client-side Web Engine rules are bypassed for the RTMP client request.
3. If HTTP headers from the origin server have the "no-cache" attribute set, content is not cached, and transparent proxy is performed to stream RTMP.
4. Transparent proxy from HTTP to RTMP is supported. Flash Media Streaming Engine begins RTMP streaming while content is still being fetched using HTTP proxy mode.

Any HTTP configuration that prevents content from being cached still applies for RTMP requests. The Flash Media Streaming Engine uses multiple HTTP-based range requests in such cases.

Multi-Bit Rate Streaming

Flash Media Streaming supports multi-bit rate streaming, also known as dynamic streaming. Dynamic streaming offers the ability to adjust the bit rate used to stream video to clients in order to adapt to changes in network conditions.

Multi-bit rate streaming has the following requirements:

- Origin server must be running Flash Media Server 3.5
- Client must be using Flash Media Player 10 or higher
- Encoder for VOD must be running Flash Media Encoder CS4
- Encoder for live streaming must be running Flash Media Live Encoder 3

For VOD, the encoder creates different bit rates for the content. For live streaming, the encoder publishes three streams with different bit rates to the origin server.

With Flash Media Player 10, there are new QoS properties that provide information about the stream and video performance and network capabilities; for example, when the NetStreamInfoBytesPerSecond field changes, the client can request a different bit rate for the stream.

See the [“Configuring Delivery Services” section on page 8-1](#) for more information about QoS.

The client player sends the command to switch or swap the stream. When network changes occur, the client sends a switch command to request the content be streamed with a higher or lower bit rate. Swap is used when swapping streams in a playlist (for example, advertisements). The bit rate change request works for both VOD and live streaming. The supported formats are H.264 and FLV. The client-side ActionScripts should use play2() instead of play() for smooth stream transitions.

Flash Media Streaming Proxy

The Flash Media Streaming Engine can deliver content acting as an origin server or as a proxy server. The Flash Media Streaming Engine acts as a proxy server when content cannot be cached due to the origin server’s configuration or due to the Service Engine’s Web Engine configuration. Content is ingested and distributed using HTTP, whether the client request for the content used HTTP or RTMP.



Note

Any content that does not contain “live” or “vod-ecds” in the path is automatically proxied.

Unicast Streaming

The Flash Media Streaming Engine supports unicast flash streaming.

Codecs

Flash Media Streaming supports the On2 VP6 codec, as well as those listed in [Table 1-3](#).

Table 1-3 Codecs Supported in Flash Media Streaming

Standard	Details
ISO/IEC 14496-3	MPEG-4 Part 3, also known as AAC+, HE-AAC. A set of compression codecs for perpetual coding of audio signals, including some variations of Advanced Audio Coding (AAC), as well as AAC Main, AAC LC, and SBR.
ISO/IEC 14496-10	Advanced Video Coding (AVC), also known as H.264/AVC. All levels of applications are supported, Base (BP), Main (MP), High (HiP), High 10 (Hi10P), and High 4:2:2 Profile (Hi422P). This standard is technically identical to the ITU-T H.264 standard.

Table 1-3 **Codecs Supported in Flash Media Streaming (continued)**

Standard	Details
ISO/IEC 14496-12	ISO Base Media File Format. A file format for storing media content containing one audio track (either ISO/IEC 14496-3 [AACPlus] or MP3), and one video track (either ISO/IEC 14496-10 [H.264 or AVC] or VP6).
3GPP TS 26.245	Time text format.

Live Streaming

Flash Media Streaming uses RTMP to stream live content by dynamic proxy. Configuration of live or rebroadcast programs is not required. When the first client requests live streaming content, the stream is created. There are no limits to the number of live streams other than the system load. Live streaming uses distributed content routing to distribute streams across multiple Service Engines.

Upon receiving a client request for live content, the edge Service Engine does the following:

- If the live stream is already present, the edge Service Engine attaches the new client to the existing stream. No message is sent to the origin server and no connection is set up.
- If the live stream is not present, ECDS creates a connection to the origin server to get the stream. No client information is sent to the origin server.

No per-client control connection is present between the edge Service Engine and the origin server for live streaming.

For Flash Media Streaming, a delivery service can be used for prefetched content, cached content, dynamically cached content, and live content. Because Flash Media Streaming uses dynamic proxy to stream live content, no disk space is used to store content. A Service Engine can act as the origin server for streaming live content, provided the SE designated as the origin server is not assigned to the delivery service that is streaming the live content.

The Flash Media Streaming Engine automatically retries a connection to an upstream Service Engine or the origin server if the upstream live-splitting connection fails. This switchover does not require any additional retries from the client side. Clients see a subsecond buffering, after which video continues to play. This feature does not address switchover when the Service Engine that is streaming to the client fails. The primary advantage is increased resiliency in the ECDS infrastructure. In other words, if a Service Engine fails, the downstream Service Engine automatically tries to connect to an upstream Service Engine in the path, and if it fails to connect, then a connection to the origin server is automatically made.

The Adobe Flash Media Encoder can publish the streams to any Adobe Flash Media Server acting as the origin server. Clients use the RFQDN to get the live content. The request from the client for “streamname” is mapped to `origin_appinst_streamname` internally in the ECDS to differentiate between two streams with the same name in two different delivery services.

**Note**

All RTMP calls for live content in the SWF file must be in the following format:

```
rtmp://rfqdn/live-ecds/path/foo.flv
```

In this format, *rfqdn* is the routing domain name of the Service Router, *live-ecds* is the required directory, and *path* is the directory path to the content file that conforms to the standard URL specification.

Flash Media Streaming supports live stream splitting. For more information about live stream splitting, see the [“Live Stream Splitting” section on page 1-12](#).

Interactive Applications

Flash Media Streaming supports pass-through (proxy) functionality for interactive applications (non-VOD and non-live). The interactive applications are hosted on a Flash Media Interactive Server that is external to the ECDS.

**Note**

For the edge server proxy to function correctly, the origin server must be running Adobe Flash Media Server 3.5.

Direct routing from the Service Engine, acting as the Flash Media Streaming edge server proxy, to the origin server (the Flash Media Interactive Server) is supported by way of the hierarchical path of Service Engines to the origin server. Every Service Engine that receives the request proxies it to the next SE along the path, where it reaches the origin server. Using the delivery service framework, the origin server is abstracted from the client request by using the Service Router Domain Name (SRDN), which resolves to the Service Engine that accepts the user connection and forwards the request to the origin server. Flash Media Streaming includes the edge server (proxy) mode, and by default, all non-live and non-VOD applications are proxied by using the edge server. Flash Media Streaming selectively picks connections for processing in edge server mode and aggregates connections to the origin servers.

**Note**

The video and audio content used in an interactive application is cached on the SE acting as the Flash Media Streaming edge server proxy and is not removed when Flash Media Streaming is disabled. The maximum storage allowed for cached content associated with interactive applications is 2 GB. The only way to delete this cached content is to use the **clear cache flash-media-streaming** command or to reload the ECDS software on the SE.

ECDS supports implicit URI as the method that allows the client to connect with the edge server without exposing the origin server. The URI would look like this: `rtmp://edge1.fms.com/ondemand`.

Request routing based on SWF files or using RTMP redirection is supported. However, RTMP redirection requires more changes in the client code. SWF file-based redirection is recommended. SWF redirection works as follows:

1. SWF files and associated HTML pages are either prefetched or hosted in the origin server.
2. Client uses a web browser to access the HTML page, which also loads the SWF file.
3. SWF file is accessed using the SRDN.
4. Service Router redirects the request to a Service Engine.
5. SWF file is downloaded to the web browser.
6. ActionScript in the SWF file attempts to connect to the same host from where the SWF file was downloaded. This is an RTMP connection that reaches the Service Engine.
7. Service Engine checks for the application type in the URI and, if it is not VOD or live, the processing is moved to the edge server mode and the connection is forwarded to the origin server.
8. Service Engine tunnels the data between the client and the origin server.

**Note**

Changes to a delivery service do not affect existing connections to the Flash Media Interactive Server (origin server). Only new connections are affected by changes to a delivery service.

Service Router

In Cisco ECDS Release 2.5.x the Service Router acts only as a Request Routing Engine, as described in the following sections:

- [Request Routing Engine, page 1-21](#)
- [Proximity Engine, page 1-28](#)

Request Routing Engine

See the following sections:

- [Routing Redirection, page 1-21](#)
- [Coverage Zone File, page 1-23](#)
- [Routing Methods, page 1-24](#)
- [Request Routing Engine Workflow of Coverage Zone Routing, page 1-26](#)
- [Request Redirection, page 1-27](#)
- [Cross-Domain Policy, page 1-27](#)

Routing Redirection

There are a number of ways for client requests to get routed to the Request Routing Engine and on to the Service Engine, including the following:

- [RFQDN Redirection](#)—Router fully qualified domain name (RFQDN) redirection.
- [IP-Based Redirection](#)—(Not supported) IP-based redirection.

RFQDN Redirection

RFQDN redirection is the default configuration. With RFQDN redirection, client requests are resolved to the Request Routing Engine by the DNS server and the Request Routing Engine redirects the request to the Service Engine based on route tables created from the [Coverage Zone File](#) and the current load of the Service Engines. The redirected URL is `http://SENAME.SE.RFQDN/relative_path_of_content`, where SENAME is the hostname of the Service Engine.



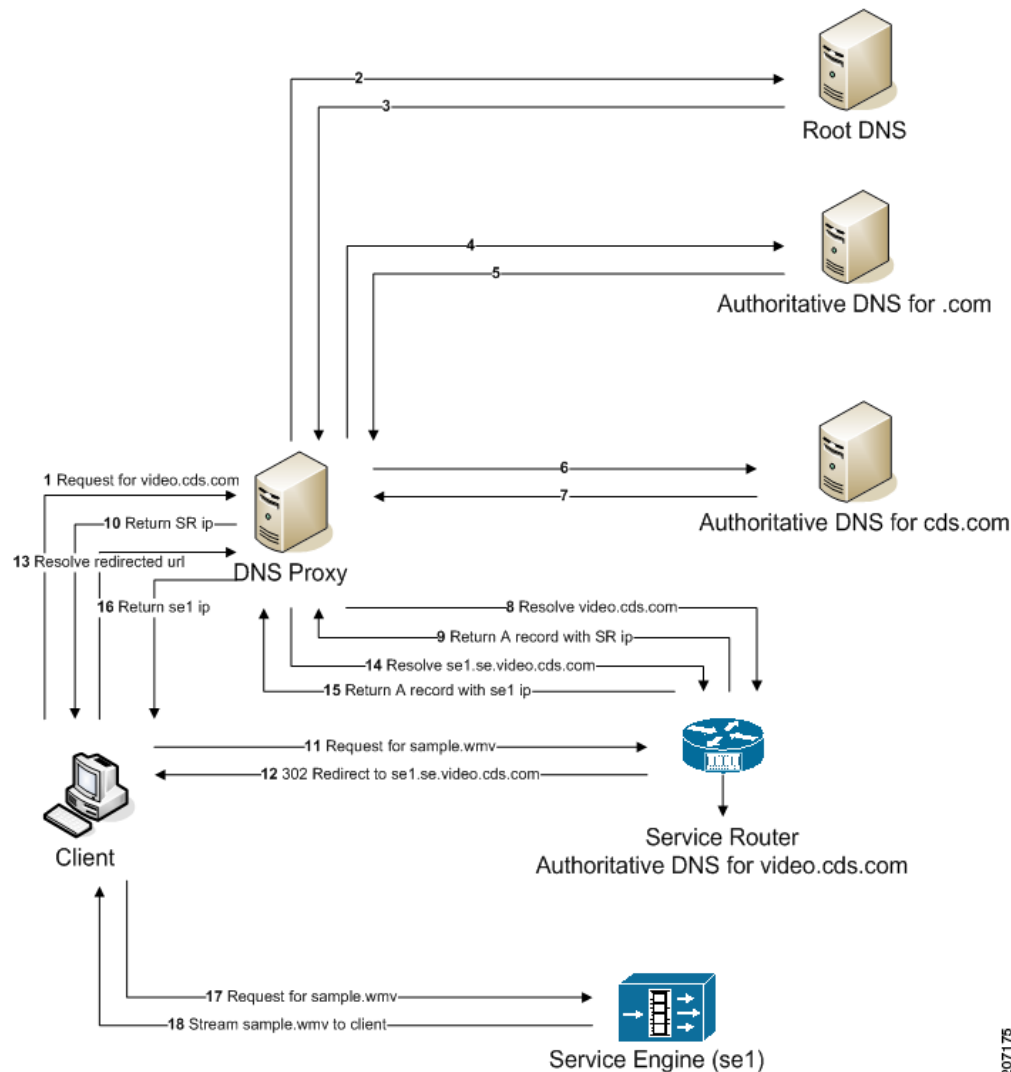
Note

The redirected URL for Flash Media Streaming requests is:

`rtmp://SENAME.SE.RFQDN/application_name/encoded (relative_path_of_streamname)`, where SENAME is the hostname of the Service Engine.

Figure 1-2 describes the Request Routing Engine workflow for RFQDN redirection.

Figure 1-2 Request Routing Engine Workflow for RFQDN Redirection



207175

In Figure 1-2, the client sends a request for a video file (for example, sample.wmv) to `http://video.cds.com`. The browser in turn sends a recursive DNS request to resolve `video.cds.com` through the DNS proxy.

The Service Router is configured to be the authoritative DNS for `video.cds.com`. The DNS proxy resolves `video.cds.com` to the Service Router's Request Routing Engine and sends the Service Router IP address back to the client. The client then sends a request for `sample.wmv` to the Service Router.

The Request Routing Engine chooses the Service Engine to redirect the request to based on load, location, and other factors. A 302 redirect message is sent to the client with the redirected URL `http://se1.se.cds.com/sample.wmv`.

A DNS request is sent to the Request Routing Engine again through the DNS proxy to resolve `se1.se.cds.com`. The Request Routing Engine returns the IP address (se1) to the DNS proxy which is forwarded to the client. The client then contacts the Service Engine (se1) directly and requests the `sample.wmv`. The Service Engine streams the requested content to the client.

IP-Based Redirection

IP-Based Redirection is not supported in this release of ECDS.

Coverage Zone File

When a Service Engine is registered to the CDSM, it is assigned a default Coverage Zone file that is created by the CDSM using the interface IP address of the Service Engine. The default Coverage Zone file can be unassigned, and a custom coverage zone can be created using the Coverage Zone file.

A Coverage Zone file is an XML file containing coverage zone entries for each client IP address range, the Service Engine serving that range, the latitude and longitude of the Service Engine, and a metric value. The Coverage Zone file can be referenced by a URL and imported into the CDSM, or uploaded from a local machine. The Coverage Zone file can be set as the default for a specific Service Router or for all Service Routers in the ECDS network.



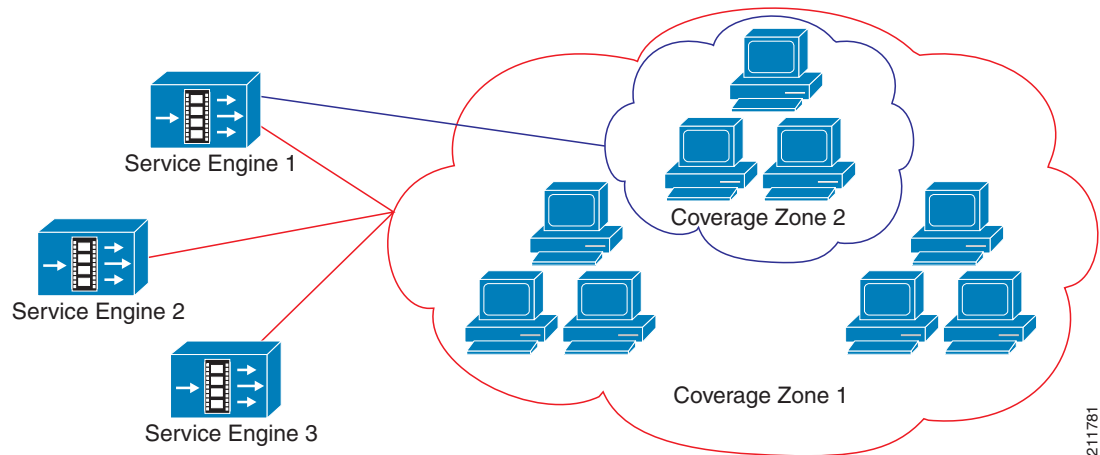
Note

The coverage zone file is limited to 40,000 entries.

When content is requested by a client, the Request Routing Engine checks the client's IP address to find the coverage zone that contains that IP address. The Request Routing Engine then selects the Service Engine that serves this coverage zone. If a specific IP address is in multiple coverage zones, the one with the more specific range is selected. If the Request Routing Engine is unable to redirect the request, the Request Routing Engine sends an error response to the client.

A coverage zone can be associated with one or more Service Engines. Each Service Engine can have its own unique coverage zone, or the Service Engines can be associated with more than one coverage zone and have overlapping coverage zones. In [Figure 1-3](#), all Service Engines serve Coverage Zone 1, and Service Engine 1 is specifically associated with Coverage Zone 2, a subset of Coverage Zone 1.

Figure 1-3 Coverage Zone Example



If a coverage zone is served by multiple Service Engines, all Service Engines are put in the routing table. The metric value, entered in the Coverage Zone file, indicates the proximity of the Service Engine to the client. When multiple Service Engines serving a coverage zone are on the same subnet and have the same metric value, and load-based routing is not enabled, the Request Routing Engine uses round-robin routing to redirect the client. If load-based routing is enabled, the load of the Service Engines are used to determine the best Service Engine to redirect the client.

For more information about Coverage Zone files, see the following sections in this guide:

- [“Coverage Zone File Registration”](#)
- [“Creating Coverage Zone Files”](#)

Routing Methods

The Request Routing Engine chooses the best Service Engine based on whether the Service Engine is participating in the delivery service for which the origin server matches that of the requested domain, and whether the Service Engine is assigned to serve the client's network region.

The Request Routing Engine uses the following methods:

- Load-based routing (least loaded)
- Last-resort routing (all Service Engines are overloaded)
- Service aware routing
- Content-based routing



Note

The keepalive messages between the Service Router and Service Engine are transmitted and received on port 2323. However, the software interoperates with older software releases that do not use port 2323 for keepalive messages. If a firewall is configured between the Service Engine and the Service Router, port 2323 (UDP) must be opened for the keepalive message to go through.

See the following sections for more information about supported routing methods:

- [Load-Based Routing, page 1-24](#)
- [Last-Resort Routing, page 1-24](#)
- [Location-Based Routing, page 1-25](#)
- [Service Aware Routing, page 1-25](#)
- [Content-Based Routing, page 1-26](#)

Load-Based Routing

Load-based routing is enabled by default and cannot be disabled. In load-based routing, the routing decision is made according to the capacity and load of the Service Engines.

The load of the Service Engine is determined by different parameters, such as processor usage, memory usage, disk usage, the number of current Windows Media streams being served, and so on. The current load is compared with the thresholds configured for the Service Engine. If a threshold has been exceeded for a Service Engine it is excluded from the routing table.

Last-Resort Routing

Last-resort routing is useful when all Service Engines have exceeded their thresholds or all Service Engines in the domain are offline, or the client is unknown. If last-resort routing is configured, the Request Routing Engine redirects requests to a configurable alternate domain when all Service Engines serving a client network region are unavailable, or the client is unknown. A client is considered unknown if the client's IP address is not part of a subnet range listed in the Coverage Zone file, or part of a defined geographical area listed in the Coverage Zone file.

Last-resort routing works dynamically. When the load of one or more Service Engines in the original host domain is reduced below threshold limits or the Service Engines are reactivated, new requests are routed to the original host domain automatically.

**Note**

If the last-resort domain is not configured and the Service Engine thresholds are exceeded, known client requests are redirected to the origin server and unknown clients either receive an error URL (if the Error Domain and Error Filename fields are configured), or a 404 “not found” message.

**Note**

Unknown clients are only redirected to the alternate domain (last-resort domain) when the **Allow Redirect All Client Request** check box is checked or the equivalent **service-router last-resort domain <RFQDN> allow all** command is entered.

Last-resort routing supports requests from RTSP, HTTP (including MMS-over-HTTP), and RTMP clients.

Location-Based Routing

Location-based routing and integration with Geo-Location servers are not supported in this release.

Service Aware Routing

Service-aware routing is enabled by default and cannot be disabled. In service aware routing, the Request Routing Engine redirects the request to the Service Engine that has the required protocol engine enabled, the required protocol engine is functioning properly and has not exceeded its threshold, and the SE has not exceeded its thresholds as configured. See the [“Setting Service Monitor Thresholds” section on page 5-97](#) for more information.

The following user agents are served by the Windows Media Engine:

- Natural Selection (NS) player and server
- Windows Media player and server

The following user agents are served by the Movie Streamer Engine:

- Quicktime player and server
- VideoLAN VLC media player
- RealMedia player

When a request reaches the Service Router, the Request Routing Engine generates a hash from the URI. The Request Routing Engine first generates a list of Service Engines to best serve the request based on service aware routing. The Request Routing Engine then reorders the list based on the hash and selects the best Service Engine. Because the hash generated for the same URI is equal, typically the same Service Engine is selected. If the Service Engine is overloaded, the next Service Engine in the list is selected.

For service aware routing, some of the services running on a Service Engine are protocol based. When protocol-based services associated with a protocol engine are stopped on a Service Engine, the Request Routing Engine excludes this Service Engine from the list of possible Service Engines that can serve requests for this type of content. The Request Routing Engine identifies the protocol engine that serves the request based on the user-agent in the request. For example, if some Windows Media Engine-related services are stopped, the Service Engine can still serve Web Engine requests. However, if the request for Web Engine content is sent from a Windows Media Player, the Request Routing Engine excludes the Service Engine from the list of possible Service Engines that can serve the request.

**Note**

For service aware routing, if a threshold is exceeded for all Service Engines, the Request Routing Engine redirects the client request to the origin server if a last-resort alternate domain is not configured. If a last-resort alternate domain is configured, the alternate domain takes precedence over the origin server. For a managed-live URL, if the origin server does not match the source of the live program, the above case fails. For the above case to work, the origin server host must be configured to match the live program source. In addition, the origin server stream name must be the same as the live program name.

Content-Based Routing

In content-based routing, the Request Routing Engine redirects the request based on the URI. Requests for the same URI are redirected to the same Service Engine, provided the Service Engine's thresholds are not exceeded.

The same content can be stored in more than one Service Engine if the number of redundant copies is set to more than one. Redundancy is used to maximize the cache-hit ratio. If redundancy is configured with more than one copy, multiple Service Engines are picked for a request with the same URI hash.

Content-based routing is best suited for cache, prefetched, and live program requests to maximize the cache-hit ratio.

**Note**

A client RTMP URL request for Flash Media Streaming does not contain the stream name; therefore, a client's URL requests for different RTMP streams could seem the same. For this reason, content-based routing may not be efficient for Flash Media Streaming because a different directory needs to be created for each stream to differentiate the content.

Request Routing Engine Workflow of Coverage Zone Routing

The Request Routing Engine workflow for clients connected to the network is as follows:

1. The client sends the DNS query for the routed FQDN to the local DNS server.
2. The DNS server replies with the Service Router IP address.
3. The client issues an HTTP, RTMP, or RTSP request to the Service Router.
4. If the Request Routing Engine finds the client's subnet in the Coverage Zone file, the following occurs:
 - a. The Request Routing Engine chooses the appropriate Service Engine and performs a protocol-specific redirection.
 - b. The client issues an HTTP, RTMP, or RTSP request to the Service Engine.
 - c. The Service Engine serves the content.

When a Service Router is registered with the CDSM, the CDSM propagates the Service Router's IP address to all the registered devices. The Service Engine sends a keep-alive message to the Service Router on a periodic interval, which consists of information about the SE resources (such as disk, CPU, memory, and network interface usage). The Request Routing Engine uses the Service Engine's load and liveness information for generating the routes.

The Enterprise CDS can have more than one Service Router to support Service Router failover. In line with failover, the DNS server should be configured with multiple Service Routers for the same routed FQDN.

**Note**

DNS entries for all FQDNs must be delegated to the Service Router. In the DNS server's database file, a name server record must be entered for each FQDN that routes to the Service Router.

Request Redirection

Table 1-4 lists supported Request Routing Engine redirections. See also the “[Content Delivery System Manager](#)” section on page 1-31.

Table 1-4 Request Routing Engine Redirections

Redirection	Description
HTTP ASX	Used if the requested file has an.asx extension. This redirection method is used for Windows Media Technology. To use the HTTP 302 redirection instead, see the “ Configuring Application Control ” section on page 6-3. Tip Normal requests for files with an .asx extension returns a status 200, unless HTTP 302 redirection is enabled.
HTTP 302	Used if the protocol is HTTP and the file extension is not .asx. This is the native HTTP redirection.
RTSP 302	Used if the protocol is RTSP and the client is QuickTime or Windows Media. This is the native RTSP redirection.
RTMP 302	Used if the protocol is RTMP and the client is Adobe Flash Player, Adobe Media Player, or Adobe Flash Lite Player.

Cross-Domain Policy

For Flash Media Streaming, when a client requests content from a portal, and the content contains a request to a different remote domain (the origin server in the case of the ECDS), the request cannot be served unless the remote domain (origin server) has a crossdomain.xml that grants access to the original portal.

For example, if a client request is for abc.com/streaming.html, and the content in streaming.html has a request to cds-origin.com/**vod-ecds**/sample.flv, the client requests a crossdomain.xml. The crossdomain.xml allows access to abc.com, which allows the streaming of sample.flv.

If the cds-origin.com does not have crossdomain.xml, then the request is denied.

**Note**

For Flash Media Streaming, the remote domain request is looked up in the crossdomain.xml file. For Microsoft Silverlight, the remote domain request is looked up in the clientaccesspolicy.xml file.

In the ECDS, instead of directly going to cds-origin.com, the request first comes to the Service Router. When the request for crossdomain.xml comes to the Service Router, the Request Routing Engine sends it to the client. This XML file grants access to the portal for the file requested. The client then sends the request for the file, which is then served.

**Note**

For Windows Media Streaming Silverlight the clientaccesspolicy.xml file is requested only when web service calls are made. Depending on the client player, for both Windows Media Streaming Silverlight and Flash Media Streaming applications, the clientaccesspolicy.xml and crossdomain.xml need to be provisioned on the origin server.

**Note**

Flash Media client players that use FLVPlaybackComponent do not currently request the crossdomain XML file for video files. The crossdomain request is issued only when a query string is present. In such cases, the video gets downloaded but does not play.

Configuring and Monitoring the Cross-Domain Policy Feature

To enable the Cross-Domain Policy feature on the Service Router, enter the **service-router access-policy enable** command.

To disable the Cross-Domain Policy feature, enter the **no service-router access-policy enable** command.

To display the Cross-Domain Policy setting, enter the **show service-router access-policy** command. The following is displayed:

```
Service Router access policy enabled
```

Logging information can be found in the /local/local1/errorlog/service_router_errorlog.current file. When the Request Routing Engine sends the crossdomain.xml to a client, the “crossdomain.xml served to client” message is logged. When the Request Routing Engine sends the clientaccesspolicy.xml file to a client, the “clientaccesspolicy.xml served to client” message is logged.

The **show statistics service-router summary** command displays an increase in the number of the HTTP Requests (normal) in Request Received section of the output.

**Note**

The crossdomain.xml or clientaccesspolicy.xml file served by the SR is logged as 200 OK, and the request redirect is logged as a 302.

Proximity Engine

Although the proximity engine settings appear in the interface and are configurable, this feature is not supported in the Cisco Enterprise CDS releases 2.5.3 through 2.5.5.

Routing Using WCCP

An alternative to Service Router routing is to use an enterprise router that supports the Web Cache Communication Protocol (WCCP) and is configured to intercept and route requests for content. WCCP detects client requests and routes the request to a Service Engine within the same network. WCCP does not require the presence of a Service Router.

WCCP is a Cisco-developed protocol that allows for the integration of web caches into the network infrastructure. It provides the mechanism to create transparent redirection of selected traffic from a group of routers to a group of web caches within the Enterprise. The main goal of WCCP is to lower response times by optimizing resource use. WCCP and transparent proxy is available for all supported media protocols in ECDS without requiring DNS or URL changes.

WCCP services are deployed for intercepting and redirecting traffic. The standard service is web cache, which intercepts TCP destination port 80 (HTTP) traffic and redirects that traffic to the cache engines. Adding more service engines and routers allows more bandwidth and flexibility in load balancing. With WCCP, you can use a “cache cluster” for load balancing, scaling, and fault tolerance.

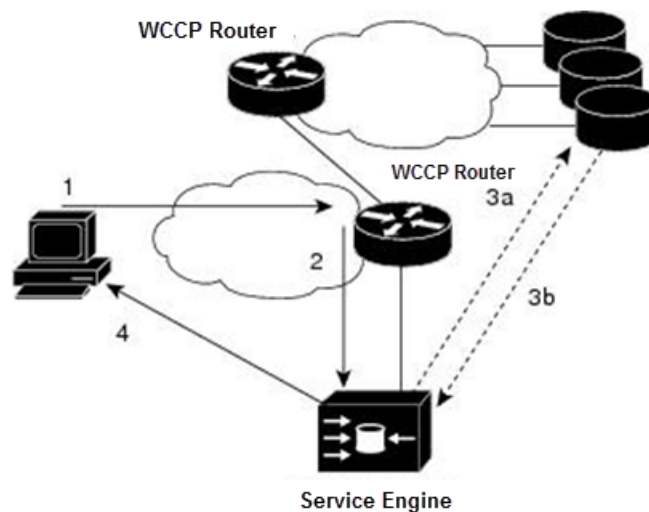
WCCP Version 2 enables a series of Service Engines, called a Service Engine cluster, to connect to multiple routers. This feature provides redundancy and a more distributed architecture for instances when a Service Engine needs to connect to a large number of interfaces. WCCP Version 2 also balances traffic load across a cache cluster and ensures fault-tolerant and fail-safe operation. As Service Engines are added to or deleted from a cache cluster, the WCCP-aware router or switch dynamically adjusts its redirection map to reflect the currently available caches.

When operating with WCCP Version 2, the Service Engine performs a clean shutdown after reboot to prevent broken TCP connections. See the [“Graceful \(Clean\) Shutdown”](#) section on page 2-20 for more information.

Figure 1-4 shows how requests for content are routed using the WCCP transparent interception method.

For more information, see [Chapter 7, “Configuring WCCP”](#) and the following sections in [Chapter 2, “Network Design”](#):

Figure 1-4 Request Interception Using WCCP



1. A user requests a web page from a browser.
2. The WCCP-enabled router intercepts the request, and based on the TCP destination port number, the router determines whether it should transparently redirect the request to a Service Engine. Access lists are used to control which requests can be redirected.
3. If the Service Engine does not have the requested content, it sets up a separate TCP connection to the origin server to retrieve the content (3a in [Figure 1-4](#)). The content returns to, and is stored on, the Service Engine (3b in [Figure 1-4](#)). Content is stored and streamed simultaneously.
4. The Service Engine sends the content to the client. Upon subsequent requests for the same content, the Service Engine transparently fulfills the request from its local storage.

WCCP can also handle asymmetric packet flows and always maintains a consistent mapping of web servers to Service Engines regardless of the number of routers used in a WCCP service group (up to 32 routers communicating with up to 32 Service Engines in a cluster).

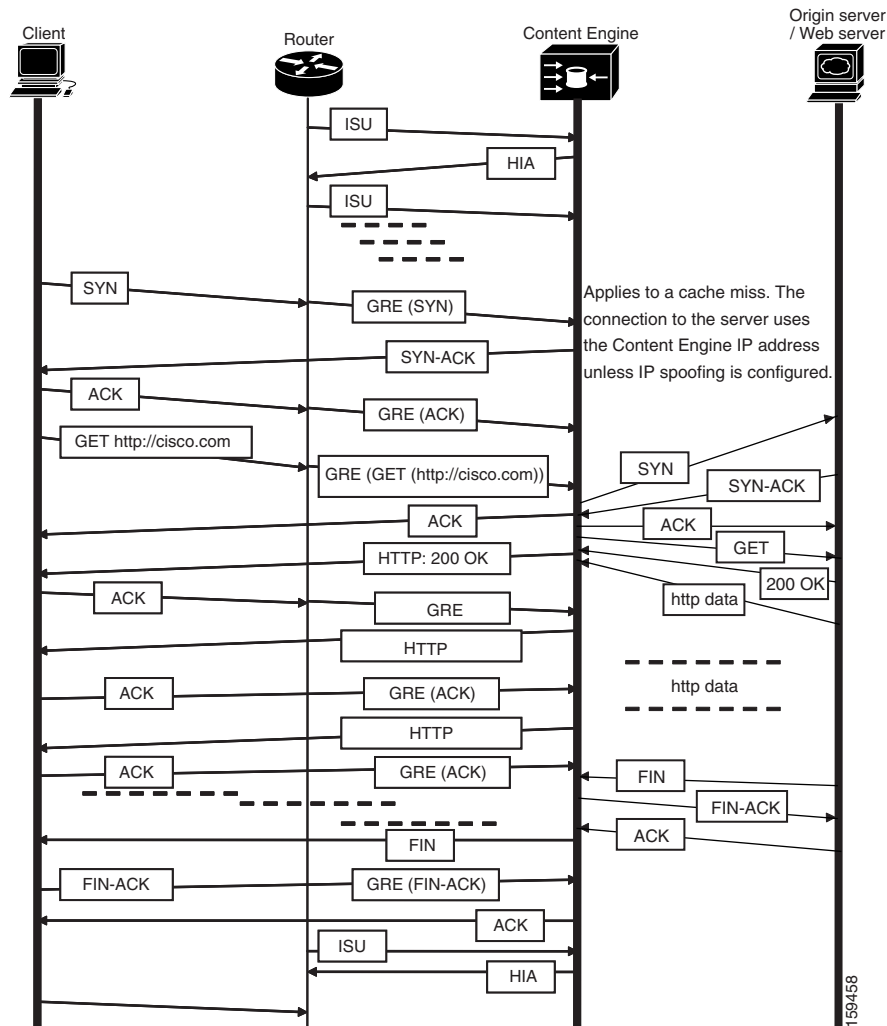
There are some significant advantages to using a WCCP-enabled router for request routing interception in transparent mode:

- No end user configuration—Users do not have to point their browsers to the Service Engine.

- Fail-safe—Service Engines are automatically fault-tolerant and fail-safe. Any Service Engine failure does not cause denial of service to the end user.
- Scalable—Cache services can be scaled by deploying multiple Service Engines.

Figure 1-5 shows the packet flow between a Service Engine and a router.

Figure 1-5 Packet Flow Diagram



In Figure 1-5, if the Service Engine does not have the requested object, a cache miss occurs, and the Service Engine sends the request to the origin server. As the Service Engine receives the response from the origin server, it saves a local copy of the requested object and delivers it to the client at the same time.

See the following sections for more information [Chapter 7, “Configuring WCCP”](#) for more information.

Content Delivery System Manager

The Enterprise Content Delivery System Manager (CDSM) is a web browser-based user interface. The Enterprise CDSM allows the administrator to configure, manage, and monitor delivery services and devices in the Cisco Enterprise Content Delivery System (ECDS). APIs are provided for backoffice integration with the Enterprise CDSM.

- [Authentication, Authorization, and Accounting, page 1-31](#)
- [Device Management, page 1-31](#)
- [Delivery Services Management, page 1-32](#)

Authentication, Authorization, and Accounting

The Enterprise CDSM uses HTTPS to secure the administrator's session. Multiple users can perform administrative operations by using the Enterprise CDSM. The administrator can configure certain users to have either view-only rights for monitoring the ECDS, or full rights that allow configuration changes as well as monitoring capabilities.

User accounts and groups can be added to the Enterprise CDSM and given roles and rights for accessing configuration information. It is also possible to segregate and group objects and give access to a limited group of users.

User authentication can be configured to use RADIUS servers when available, otherwise the Enterprise CDSM provides its own authentication server.

The ECDS-wide policy and status information is maintained in a relational database on the Enterprise CDSM. This information is propagated and synchronized with all devices in the ECDS network.

As part of the network management process, the administrator can perform basic administration operations on the Enterprise CDSM database, including backup and restore.

Device Management

The Enterprise CDSM sends device configuration changes to the selected device or group of devices once the change has been submitted. The device sends any configuration changes that were made locally to the CDSM, and also provides periodic status information.

Devices can be organized into user-defined device groups, which allow administrators to apply configuration changes and perform other group operations on multiple devices simultaneously. Because a device can belong to multiple device groups, this reduces the management overhead of the administrator. Device groups allow for a single instance of management thus eliminating the need to repeat the same step for each device.

The Enterprise CDSM also provides an automated workflow to apply software upgrades to the devices in a device group.

Higher Storage Utilization of ECDS

Storage across multiple Service Engines is virtually divided into buckets where each Service Engine serves only a subset of the total content. Both the local storage and RAM of the Service Engines can function as an aggregated distributed service, providing unlimited scalability. Linear scaling of the ECDS storage is accomplished by adding more Service Engines to one location. This addresses the demands of the "Long Tail" use case relevant to the Service Engines. The Long Tail is the realization

that the sum of many small markets is worth as much, if not more, than a few large markets. Long-tail distribution is the possibility that extremely infrequent occurrences in traffic are more likely than anticipated.

This higher storage utilization provides the following:

- Overall better system performance
- Higher in-memory cache hit ratio
- Deterministic resiliency in case of failures or overload due to very popular content (This is useful when customers have live, prefetched, and cached assets more than 4.5 terabytes of content on one Service Engine.)

The content distribution is resilient and stateless. If the load of all content mapped to one Service Engine increases, the load is automatically spread to other Service Engines without requiring any administrator intervention.

Delivery Services Management

The Enterprise CDSM provides the configuration and monitoring of delivery services, which defines how content is ingested, stored, cached, and published. The Enterprise CDSM provides the Service Engines with information about the delivery services and which Service Engines are participating in the delivery service.

In addition to using the Enterprise CDSM to define delivery services, an XML file called a *Manifest file* can be used to define a delivery service. The Manifest file and APIs serve as the basis for backoffice integration. For more information about the Manifest file, see the [“Manifest File” section on page 2-10](#).

Resiliency and Redundancy

An ECDS that is designed with full redundancy and no single point of failure includes redundant Enterprise CDSMs and Service Routers. The redundancy mechanisms for the Content Acquirer and Media Streamer applications running on the Service Engines operate differently.

- [Content Acquirer Redundancy, page 1-32](#)
- [Media Streamer Redundancy, page 1-33](#)
- [Service Router Redundancy, page 1-33](#)
- [Enterprise CDSM Redundancy, page 1-33](#)

Content Acquirer Redundancy

In the event of a primary failure on the Content Acquirer, the failover mechanism supports the election of a backup Content Acquirer. A failover requires that both the primary and backup Content Acquirer be located in the root location of the delivery service.

Live Programs

If the Content Acquirer receives a live program as a multicast stream from the origin server, upon failure of the primary, the backup Content Acquirer assumes control of that program’s streaming and the program continues without interruption. This process is transparent to the end user. When the primary

Content Acquirer comes back online, it receives the live stream from the active secondary Content Acquirer and does not fall back (regain its primary status) until the live program has finished or has been restarted.

If the Content Acquirer receives the program as a unicast stream from the origin server, the failover mechanism is not supported. If the primary Content Acquirer fails while a program is playing, the person viewing the program must re-request the program.

Media Streamer Redundancy

If a Service Engine running the Media Streamer application fails, the Service Router stops receiving keep-alive messages from that Service Engine. When a new request comes in, the Service Router does not redirect the request to that Service Engine; instead, it redirects the request to other Service Engines within the same delivery service. All the existing sessions on the failed Service Engine terminate and the affected end users must re-request the content.

Service Router Redundancy

If the ECDS network is designed with multiple Service Routers, all Service Routers are aware of all Service Engines in the ECDS. The DNS servers must be configured with multiple Service Routers and the failover is handled by the DNS servers.

Enterprise CDSM Redundancy

The Enterprise CDSM can operate in two different roles: primary and standby. The primary role is the default. There can only be one primary active in the ECDS network; however, you can have any number of Enterprise CDSMs operating in standby to provide redundancy and failover capability.

Primary and standby CDSMs must be running the same version of software. We recommend that the standby CDSM be upgraded first, followed by the primary CDSM.

The Enterprise CDSM design principle is that the management device is never in the service delivery path. When the CDSM fails, the rest of the ECDS continues to operate. A CDSM failure does not affect any services delivered to end users, and all content ingest continues. The only negative effect is that the administrator cannot change configurations or monitor the ECDS. As soon as a failure to connect to the CDSM is noticed, the administrator can activate the standby CDSM. For information on making the standby CDSM the primary CDSM, see the [“Changing a Standby to a Primary Enterprise CDSM” section on page 3-12](#).

Where to Go Next

Proceed to [Chapter 2, “Network Design”](#) for information about the basics of provisioning a Cisco ECDS network and how metadata and content flow through the Cisco ECDS.



Tip

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Configuration Guide on Cisco.com.



CHAPTER 2

Network Design

The following sections describe the basics of provisioning a Cisco ECDS network and how metadata and content flow through the Cisco ECDS:

- [Provisioning the Cisco ECDS, page 2-1](#)
- [Cisco ECDS Topology, page 2-2](#)
- [Delivery Service, page 2-3](#)
- [Workflow Diagrams, page 2-12](#)
- [WCCP Services, page 2-15](#)
- [HTTP and HTTPS Support, page 2-22](#)
- [Programs, page 2-27](#)
- [Where to Go Next, page 2-28](#)



Note

To achieve the best throughput, we recommend you configure a port channel for the two gigabit Ethernet interfaces on the SE.

Provisioning the Cisco ECDS

Provisioning the Cisco ECDS consists of two main tasks.

Task	Action
1.	Register the devices to the Enterprise CDSM and define the network topology and device groups.
2.	Configure the delivery services that deliver content to the clients.

Cisco ECDS Topology

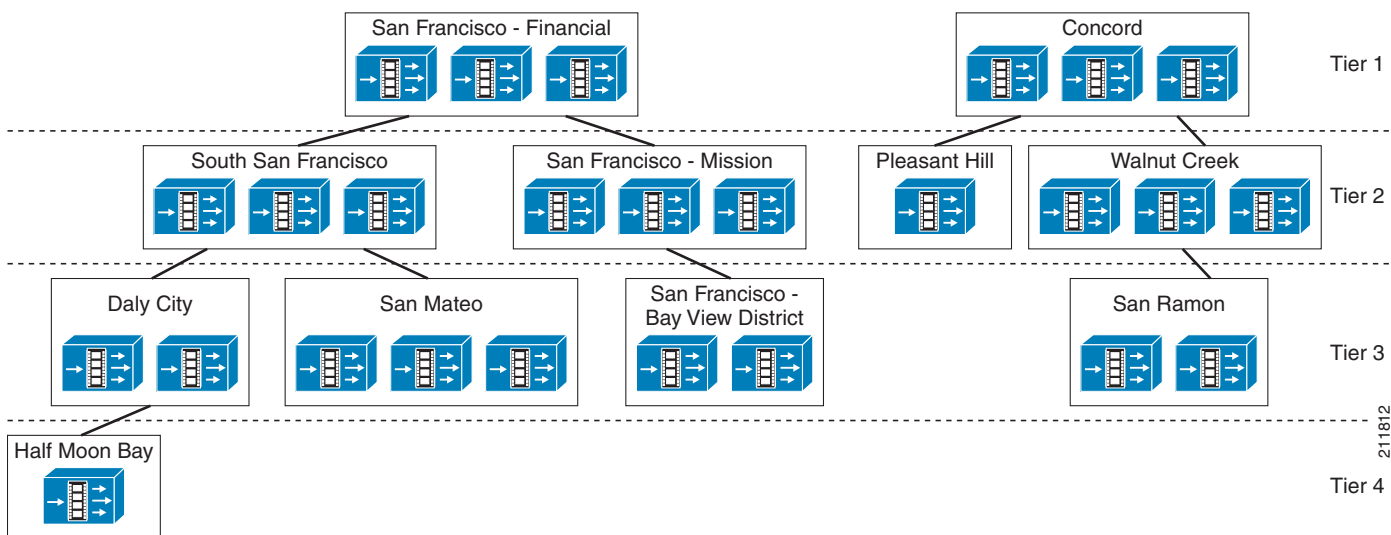
In the Cisco ECDS Service Engines are grouped together into locations, and a set of locations is then organized into the form of a tree, called a “Location Tree.” The Location Tree represents the network topology configuration that is based on parent-child relationships. Locations are well connected and have similar connectivity properties to the outside world. A location generally implies topological proximity. Each location can have a parent relationship and multiple child relationships, such that each location can have zero to one parent locations and zero to many child locations. These relationships guide how content flows among locations but does not restrict content flow in any direction.

Locations are also classified into tiers. Each tier consists of locations belonging to the same tier. All locations with no parents belong to Tier 1. All locations that are children of Tier 1 locations belong to Tier 2.

The Cisco ECDS can consist of one or more topological Location Trees. A Cisco ECDS network is limited by the maximum depth of four tiers.

Figure 2-1 illustrates two location trees, with the parent-child relationship of each location indicated by a solid line and each tier indicated by a dotted line.

Figure 2-1 Location Trees Example



The Location Trees define preferred distribution routes. The Tier 1 locations are located closest to the WAN backbone. Tier 1 locations can communicate with all other Tier 1 locations.



Note

The ECDS does not support network address translation (NAT) configuration, where one or more SEs are behind the NAT device or firewall. The workaround for this, if your ECDS network is behind a firewall, is to configure each internal and external IP address pair with the same IP address.

The ECDS does support clients that are behind a NAT device or firewall that have shared external IP addresses. In other words, there could be a firewall between the ECDS network and the client device. However, the NAT device or firewall must support RTP/RTSP.

Device Groups

Device groups offer a way to group similar devices and configure all the devices in a group at one time. Service Engines can be assigned to multiple device groups when the Device Group Overlap feature is enabled.

A device in a device group can have individual settings different from other devices in the group, and its settings can revert back to the group settings. The last configuration submitted for the device, whether group or individual, is the configuration the device uses.

In addition to group configuration and assignment, the CDSM allows the following:

- Hiding configuration pages of a device group
- Adding all newly activated devices to a device group
- Forcing device group settings onto all devices assigned to a group

A device can be assigned to a device group in one of two ways:

- From the Device Assignment page
- From the Device Group Assignment page

Baseline Groups

A baseline group denotes a group of devices for a particular service. There are three baseline groups:

- Web Baseline Group—Used for web-based content
- Video Baseline Group—Used for video content
- Platform Baseline Group—Used for platform-specific configurations

A device group can be configured as a baseline group. A device can be assigned to a baseline group in the following three ways:

- From the Devices home page
- From the Device Assignment page
- From the Device Group Assignment page

Delivery Service

A delivery service is a configuration that defines how content is acquired, distributed, and stored in advance of a client request (prefetch), and after a client request (cached). Content from a single origin server is mapped to a set of Service Engines by a delivery service. Content objects associated with a specific delivery service have a common domain name; in other words, the content in a specified delivery service resides in a single location on an origin server. Each delivery service maps service routing domain names to origin servers one-to-one for Service Router DNS interception.

The CDSM is used to create the topology and configure the delivery services. All Service Engines and Service Routers that register with the CDSM are populated with the topology and the information about the configured delivery services.

The designated Content Acquirer is the only role which is administratively defined in the CDSM, all other roles, based on the topology and delivery service subscription, are assumed by the Service Engines automatically.

Both prefetched content and on-demand (dynamic and hybrid) content caching is supported. Different algorithms are used to elect the Service Engines for the various roles based on the type of content being distributed.

See the following sections for more information:

- [Content Acquirer, page 2-4](#)
- [Location Leader, page 2-5](#)
- [Forwarder and Receiver Service Engines, page 2-6](#)
- [Persistent HTTP Connections, page 2-7](#)
- [Network Partition, page 2-8](#)
- [Delivery Service Distribution Tree, page 2-8](#)
- [Types of Delivery Services, page 2-9](#)
- [Methods for Ingesting Content, page 2-9](#)

Content Acquirer

For each delivery service, there is only one Content Acquirer but multiple Service Engines. The location that has the Content Acquirer for a delivery service is called the *root location*. Other Service Engines in the root location that are assigned to the same delivery service can act as backup Content Acquirers if the configured Content Acquirer fails.



Note

The locations can be virtual. For example, a location can consist of the enterprise data center and the backup data center. The SEs in both the data center and the backup data center can be backup Content Acquirers for each other.

For Content Acquirer redundancy, a delivery service must have at least two SEs located in the root location. If the primary Content Acquirer fails or becomes overloaded, the SEs in the delivery service use the selected backup Content Acquirer (there could be several SEs assigned to the delivery service that are colocated at the root location).

See the following sections for more information:

- [Content Acquirer Selection for Prefetched Content, page 2-4](#)
- [Content Acquirer Selection for Dynamic or Hybrid Ingest, page 2-5](#)

Content Acquirer Selection for Prefetched Content

For prefetched content, the designated Content Acquirer always performs the content acquisition. Only in an event of a failure does another Service Engine in the same location assume the Content Acquirer role.

The selection algorithm runs in every Service Engine in the root location (also known as the Content Acquirer location). The algorithm always runs in context of a delivery service; that is, only the Service Engines subscribed to the same delivery service are considered in the selection.

Each Service Engine creates an ordered list of Service Engines belonging to the same location and subscribed to the same delivery service. In the root location, the designated Content Acquirer is always added as the first entry in the list.

At steady state when there are no failures, the designated Content Acquirer performs the content acquisition. Each Service Engine in the delivery service gets the content and metadata from the Content Acquirer by way of forwarder Service Engines and receiver Service Engines. Every Service Engine polls its forwarder Service Engine periodically for content and metadata. For more information, see the [“Forwarder and Receiver Service Engines” section on page 2-6](#).

In the event that the Content Acquirer fails, the periodic polls for metadata fail causing the Service Engines to run the Content Acquirer election algorithm.

Each Service Engine creates the ordered list again. The list looks the same as the previous list, except that the Content Acquire which just failed is not considered in the election process. The Service Engine that appears second in the ordered list now assumes the role of the Content Acquirer.

Content Acquirer Selection for Dynamic or Hybrid Ingest

For on-demand content, which is dynamic or hybrid ingest, the designated Content Acquirer is only used to determine the location of where to acquire the content from the origin server directly. All of the Service Engines in the root location are eligible to acquire the content. The Service Engine selected to acquire the content is based on a URL hash. Content acquisition and storage is spread across multiple Service Engines.

The selection algorithm runs on every Service Engine in the root location (also known as the Content Acquirer location). The algorithm always runs in context of a delivery service; that is, only Service Engines subscribed to the same delivery service are considered in the selection.

Each Service Engine creates an ordered list of Service Engines belonging to the same location and subscribed to the same delivery service. This ordering is based on a index created by a URL hashing function. At steady state when there are no failures, the Service Engine that appears first in the list performs the content acquisition.

In addition to the URL-based list ordering, the health and the load of the Service Engines are also considered in the selection. Service Engines that do not have the applicable protocol engine enabled, failed Service Engines, and Service Engines with load thresholds exceeded are eliminated from the selection process. If a Service Engine is eliminated from the list, the next Service Engine in the ordered list is used to acquire the content.

See the [“Specifying Hybrid Ingest Content” section on page B-15](#) for more information.

Location Leader

All other locations (that is, non-root locations) in the delivery service have an SE designated as the *location leader*. The location leader is determined automatically by the CDSM. The other SEs act as backup location leaders in case the location leader fails. In the same location, different delivery services may have different SEs as their location leaders. The location leader gets the delivery service content from outside the location, while the other SEs in the location get the content from the location leader. This reduces the distribution traffic on low-bandwidth links, because the SEs in the same location are likely to be on the same LAN.

Use the **show distribution forwarder-list** and **show distribution location location-leader-preference** commands to see the location leader for a delivery service.

See the following sections for more information:

- [Location Leader Selection for Prefetched Content, page 2-6](#)
- [Location Leader Selection for Live Streaming, page 2-6](#)
- [Location Leader Selection for Dynamic or Hybrid Content, page 2-6](#)

Location Leader Selection for Prefetched Content

The location leader selection for prefetched content is based on the same algorithm that is used for the Content Acquirer backup selection for prefetched content, except that the Service Engines are ordered based on an internal ID assigned at the time of registering to the CDSM. The first Service Engine in the list is selected. In the root location, the designated Content Acquirer is always the location leader.

Location Leader Selection for Live Streaming

For live streaming, the location leader selection is based on the program URL hash and the service availability. Each program within a delivery service could have different location leaders. Depending on the URL hash and the number of SEs in the location, some SEs could be acting as the location leader for more than one program.

Location Leader Selection for Dynamic or Hybrid Content

For on-demand content, which is dynamic ingest or hybrid ingest, the location leader selection is based on the same algorithm that is used for the Content Acquirer selection for on-demand content, with the algorithm repeated for each location. This mechanism helps distribute the load, improve cache hits, and reduces redundant content (which contributes to storage scalability). The location leader selection is very similar to how a location leader is selected for live streaming content.

Forwarder and Receiver Service Engines

Content distribution flows from the Content Acquirer to the receiver Service Engine (SE) by way of store and forward. A *receiver* SE does not just go directly to the Content Acquirer for content. Rather, it finds out who its upstream SE (the *forwarder* SE) is and pulls the content from that forwarder. The forwarder SE in turn pulls the content from its own forwarder, which may be the Content Acquirer. All receiver SEs store the content on disk after they get the content. Each receiver SE selects a forwarder SE.

The store-and-forward process causes content to flow through a distribution tree constructed specifically for this delivery service and with all receiver SEs in the delivery service as nodes on the tree. If an SE does not belong to the delivery service, it does not appear on the tree.

Both the metadata about the content and content itself flow through the distribution tree. This tree is constructed by using the dynamic routing of the delivery service and is often a subtree of the overall ECDS topology.

Although the tree is global, the delivery service routing process is actually a per-SE local function that answers the question “who is my forwarder for this delivery service?”

The following criteria is used to select a forwarder:

- An SE is a forwarder for other SEs in its own location if it subscribes to the delivery service and it is the location leader for the delivery service.
- An SE in location A can be a forwarder for SEs from location B if it subscribes to the delivery service, location A is “closer” to the root location of the delivery service than location B, and there is no other location between location A and location B that has a receiver SE of the delivery service. When selecting a forwarder from other locations, a receiver SE uses a hash algorithm seeded with its own unique SE ID (assigned by the CDSM), to spread the load of multiple receivers equally to all eligible forwarders.

**Note**

A “location leader” is always a per-delivery service and per-location concept, while a “forwarder” is always a per-delivery service and per-SE concept.

A receiver SE finds its forwarder by examining the series of locations on the topology “toward” the root location, following the parent-child relationship as described in the [“Cisco ECDS Topology” section on page 2-2](#).

1. First, find a forwarder within the SE's own location. The location leader should be the forwarder. If the location leader is down, use the backup location leader as the forwarder.
2. If none is found or if the SE thinks it is the location leader, look for a forwarder in the next location “toward” the root location. If still none are found (for example., there is no SE at that location assigned to the delivery service or the potential ones are unreachable), then look further “toward” the root location, and so on. The recursion ends if a forwarder is found or the Content Acquirer's location is reached.
3. Multicast Forwarder: If the delivery service is marked “multicast enabled,” the delivery service searches for a multicast forwarder. If it fails to find any reachable multicast forwarder, it searches again, this time, looking for unicast forwarders.
4. Content Acquirer failover: If the SE is unable to find a live forwarder (for example, there is a network or machine outage), the SE has to retry later, unless it is in the root location for the delivery service and is allowed to failover to the origin server directly and act as a backup Content Acquirer.

**Note**

This process follows the search path provided by the overall topology that was configured for the ECDS. Using the combination of the overall topology configuration and the assignment of SEs to delivery services, the ECDS gives the administrator a lot of control over the form of the distribution tree, and yet still automates most of the selection and failover process.

Persistent HTTP Connections

HTTP connections are maintained among the SEs in a delivery service and the origin server as long as the connection idle period does not exceed the keepalive timeout period of 30 seconds or the idle period does not exceed the timeout period set on the origin server, whichever is the shorter period.

Persistent HTTP connections in a delivery service work in the following way:

1. **Open new HTTP connection.** The first time a request for cache-miss content is sent to an upstream device (SE or origin server), which is identified by the IP address of the device, a new HTTP connection is formed.

The Web Engine has 8 working threads, which are computing units. Each thread can have as many connections to as many upstream devices as required.

There are a maximum of 10 connections per upstream device (SE or origin server) that are persisted in the idle queue for reuse for each of the 8 working threads, which gives a total of 80 persistent connections.

2. **Connection moved to idle queue.** Once the content download is complete, the connection is moved to the idle queue.

3. **Closing connections in idle queue.** A 30-second keepalive timeout period is applied to each connection moved to the idle queue and if the idle time of a connection reaches the keepalive timeout period, it is closed. If a new request needs to be sent and there is a connection for the same server (IP address) in the idle queue, the connection is moved to the main connection list and used for that request.
A working thread uses an existing connection if the connection is idle; otherwise, a new connection is opened.
4. **Open and close non-persistent connection.** If a request for cache-miss content needs to be sent and there are no idle connections for that upstream device, a new connection is created. If, after the request is served, there already exists 10 connections for the upstream device in the idle queue, the connection is terminated.
5. **Close 50 percent of connections in idle queue.** If the origin server has a timeout period for HTTP connections, that is taken into consideration. The 30-second keepalive timeout is used for closing old HTTP connections. If the upstream SE or origin server has a shorter keepalive timeout period, that takes precedence over the downstream SEs 30-second keepalive timeout. If there are no keepalive timeout values set on the upstream devices (SEs or origin server), then every 30 seconds 50 percent of the persistent connections (maximum of 80 per origin server) are closed.

Network Partition

In the case of network partitions, there can be multiple Content Acquirers for a single delivery service, or multiple location leaders. There can be as many Content Acquirers as there are network partitions (that have backup Content Acquirers) in the root location. Once the partition incident is over in the root location, the system recovers and there is only one Content Acquirer again. There can be as many location leaders as there are partitions (that have subscriber SEs) in any location. Once the partition incident is over, the system recovers from it and there is one location leader again.

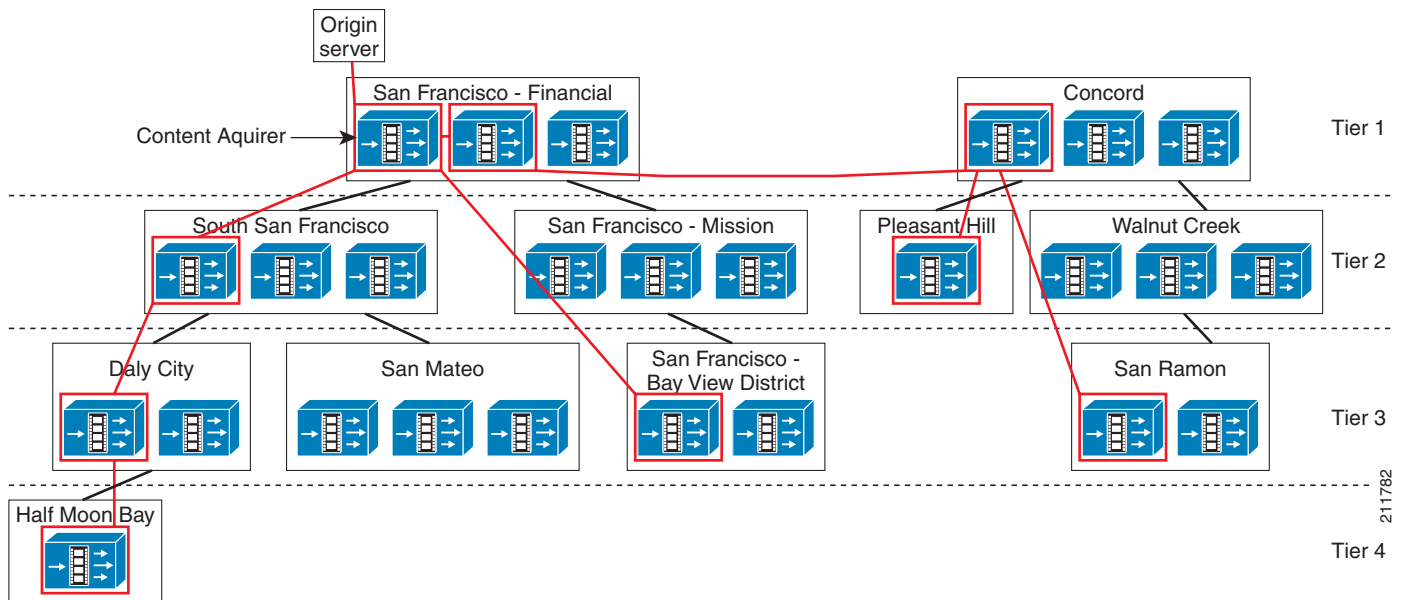
Delivery Service Distribution Tree

Delivery services form logical routes for content to travel from an origin server through the Content Acquirer to all the Service Engines in the delivery service. Logical routes for content distribution are based on the device location hierarchy or Location Tree.

The content distribution route follows the general tree structure of the Location Tree, where content is distributed from the root of the tree (Content Acquirer) to the branches (Service Engines associated with the delivery service). A delivery service distribution tree is constructed for each delivery service.

By excluding it from the Coverage Zone file, a Service Engine in a delivery service can be configured only to forward content and metadata, and not deliver the content to client devices.

Figure 2-2 shows an example of a delivery service distribution tree. The Service Engines participating in the delivery service are marked in red. Possible content and metadata routes are indicated by red lines. The actual route may differ among the participating Service Engines as determined by the Service Router routing method.

Figure 2-2 Delivery Service Distribution Tree Example

Types of Delivery Services

The Cisco ECDS supports two types of delivery services:

- [Prefetch/Caching Delivery Services, page 2-9](#)
- [Live Delivery Service, page 2-9](#)

Prefetch/Caching Delivery Services

For prefetch delivery services, called content delivery services in the CDSM, content is forwarded from Service Engine to Service Engine through the delivery service distribution tree until all Service Engines in the delivery service have received it. The delivery service distribution architecture provides unicast content replication using a hop-by-hop, store-and-forward methodology with the forwarder Service Engines systematically selected on the basis of the manually configured location hierarchy. For caching delivery services, the content need not be fully stored before forwarding.

Live Delivery Service

The live delivery services are only used for managed live stream splitting. The prefetch/caching delivery services are used for prefetch ingest, dynamic ingest, and hybrid ingest.

Methods for Ingesting Content

There are two methods that can be used to configure a delivery service:

- Specifying the content by using an externally hosted Manifest file.
- Specifying the content by using the Enterprise CDSM.

The Enterprise CDSM provides a user-friendly interface for adding content and configuring crawl tasks. All entries are validated and a Manifest file is generated. The Enterprise CDSM offers the most frequently used parameters, a subset of the Manifest parameters. For a complete set of parameters, use a Manifest file.

The following sections describe the main building blocks of a delivery service:

- [Origin Servers](#)
- [Manifest File](#)
- [Content Acquirer](#)
- [Media Streamer](#)

Origin Servers

Content is stored on origin servers. Each delivery service is configured with one content origin. The same origin server can be used by multiple live delivery services. However, only one prefetch/caching delivery service is allowed per content origin. Each Content Origin is defined in the Enterprise CDSM by the following:

- Origin server
- Service routing domain name

The origin server is defined by the domain name that points to the actual origin server. The origin server domain name is used to fetch content that resides outside the delivery service, and to request redirection in case of a failure. The origin server must support at least one of the following protocols in order for the ECDS to be able to ingest content:

- HTTP
- HTTPS
- CIFS
- SMB

Content can also originate from a local file on the ECDS.

The service routing domain name is an FQDN and is used for content redirection. Each content that is ingested by the Manifest file is published using the service routing domain name. The service routing domain name configured for the Content Origin must also be configured in the DNS servers, so client requests can be redirected to a Service Router for request mediation and redirection.

Proxy Server

When the Content Acquirer cannot directly access the origin server because the origin server is set up to allow access only by a specified proxy server, a proxy server can be configured. The proxy server is configured through the Enterprise CDSM for fetching the Manifest file, and through the Manifest file for fetching the content. Proxy configurations made in the Manifest file take precedence over proxy configurations in the CLI.

Manifest File

The Manifest file contains XML tags, subtags, and attributes used to define how content is ingested and delivered. Each delivery service has one Manifest file. The Manifest file can specify attributes for content playback and control. Attributes for specifying metadata only, without fetching the content, are supported. If special attributes are set, only the metadata and control information are propagated to the

Service Engines. The control data is used to control the playback of the content when it gets cached by dynamic ingest. The Manifest file format and details are described in [Appendix B, “Creating Manifest Files.”](#)

Crawling

For HTTP, HTTPS, SMB, or CIFS, a single item can be fetched by specifying a single URL in the CDSM or Manifest file, or content can be fetched by using the crawler feature. The crawler feature methodically and automatically searches acceptable websites and makes a copy of the visited pages for later processing. The crawler starts with a list of URLs to visit, identifies every web link in the page, and adds every link to the list of URLs to visit. The process ends after one or more of the following conditions are met:

- Links have been followed to a specified depth.
- Maximum number of objects has been acquired.
- Maximum content size has been acquired.

The crawler works as follows:

1. The Content Acquirer requests the starting URL that was configured for the delivery service.
2. The crawler parses the HTML at that URL for links to other files.
3. If links to other files are found, the files are requested.
4. If those files are HTML files, they are also parsed for links to additional files.

In this manner, the Content Acquirer “crawls” through the origin server.



Note

The crawler cannot parse JavaScript or VBScript to get the links, nor does it work with HTTP cookies.

A website that has indexing enabled and the default document feature disabled generates HTML that contains a directory listing whenever a directory URL is given. That HTML contains links to the files in that directory. This indexing feature makes it very easy for the crawler to get a full listing of all the content in that directory. The crawler searches the folders rather than parsing the HTML file; therefore, directory indexing must be enabled and the directory cannot contain index.html, default.html, or home.html files.

Content ingest from an SMB server for crawl jobs crawls the folder hierarchy rather than parsing the HTML file.

Content Acquirer

The Content Acquirer parses the Manifest file configured for the delivery service and generates the metadata. If the hybrid ingest attributes are not specified, the Content Acquirer ingests the content after generating the metadata. The Content Acquirer can be shared among many delivery services; in other words, the same Service Engine can perform the Content Acquirer role for another delivery service.

SMB Servers

The ECDS supports file acquisition from Windows file servers with shared folders and UNIX servers running the SMB protocol. The Content Acquirer first mounts the share folder. This mount point then acts as the origin server from which the content is fetched. The Content Acquirer fetches the content and stores it locally.

**Note**

With SMB, files greater than two gigabytes cannot be ingested.

HTTP(S) Servers

The no-cache directive in an HTTP(S) server response header tells the client that the content requested is not cacheable. When an HTTP(S) server responds with a no-cache directive, the Content Acquirer behaves as follows:

- If the content to be ingested is specified in an <item> tag in the Manifest file, the Content Acquirer ignores the no-cache directive and fetches the content anyway.
- If the content to be acquired is specified in a <crawler> tag in the Manifest file, the Content Acquirer honors the directive and does not fetch the content.

Media Streamer

The Media Streamer application on the Service Engine participates in the delivery service by distributing content within the ECDS and delivering content to the clients. The Service Engines can be shared among other delivery services.

HTTP(S) Download—Disabling

In some instances, for example when there are contractual obligations to prevent clients from downloading content, it may be necessary to disable HTTP(S) downloads on a delivery service. When HTTP(S) download is disabled, the Web Engine returns a 403 forbidden message. For configuration information, see the [“Creating Delivery Service” section on page 8-4](#).

Workflow Diagrams

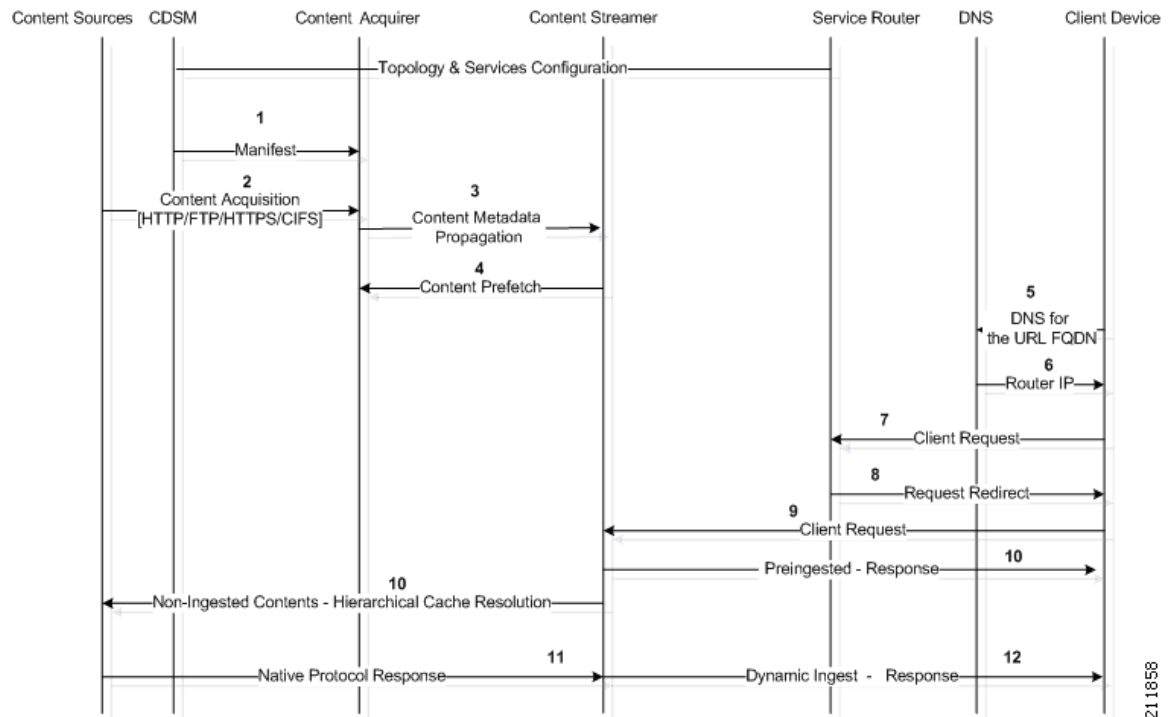
The following diagrams describe ECDS content workflows:

- [Content Request Using the Service Router, page 2-13](#)
- [Content Request Using WCCP, page 2-15](#)

Content Request Using the Service Router

Figure 2-3 shows the delivery service workflow.

Figure 2-3 Delivery Service Workflow Acquisition and Playback Diagram



Service Workflow Example Details

1. The topology is propagated to all the devices registered and activated in the Enterprise CDSM. The delivery service configuration is propagated to all the Service Engines subscribed to the delivery service. The Manifest file information is sent to the Content Acquirer for the delivery service.
2. The Content Acquirer parses the Manifest file and generates the metadata. All content listed in the Manifest file, except for non-cache content types, is fetched.
3. The Content Acquirer propagates the metadata to all other Service Engines.
4. The Service Engines receive the metadata and associated prefetched content. The Service Engines do not prefetch content that is “wmt-live” or “cache” types. The “wmt-live” type corresponds to the Windows Media live streaming and the “cache” type corresponds to the hybrid ingest content.
5. The client request for a URL first performs a DNS resolution. The Service Router is configured as the authoritative DNS server for the hosted, or service routing, domain. The URLs that are published to the users have the service routing domain names as the prefix.
6. The Service Router resolves the service routing domain name to its own IP address.
7. The client sends the request to the Service Router and the Service Router uses its routing method to determine the best Service Engine to stream the requested content.
8. The Service Router redirects the client to the best Service Engine.
9. The client sends the request to the Service Engine.

The following are the possible scenarios after the request reaches the Service Engine:

- **Prefetched/Pinned Content**

Flow 10, “Pre-ingested response.”

The content is prefetched using the URL: <http://www.ivs-example.com/video/wmv-152>

The actual user request is: <http://cr-video.example.com/video/wmv-152>

The Service Engine processes the user request, and based on the metadata, determines the content was prefetched and pinned in its local storage. The Service Engine looks up the policies for the content and streams the content to the user.

- **Dynamic Ingest/Cached Content**

Flows 10, 11, 12, “Non-ingested contents—Hierarchical cache resolution,” “Native Protocol Response,” and “Dynamic ingest response.”

If the request for content is not specified in the Manifest file, dynamic ingest is used.

The user request is: <http://cr-video.example.com/video/wmv-cached.wmv>

The Service Engines in the delivery service form a hierarchy, pull the content into the ECDS, and cache it. The Service Engine streams the content to the user.

- **Hybrid Ingest/Metadata Only Content**

(no content flow)

The request for content is specified in the Manifest file as “cache.”

The user request is: <http://cr-video.example.com/video/wmv-59>

The Service Engine fetches the content, similar to the dynamic ingest method, but the metadata attributes (for example, `serveStartTime`, `serveStopTime`) are honored by the Service Engines and the content is served only if the request falls within the defined time interval.

Table 2-1 shows sample values for the delivery service workflow described in Figure 2-3.

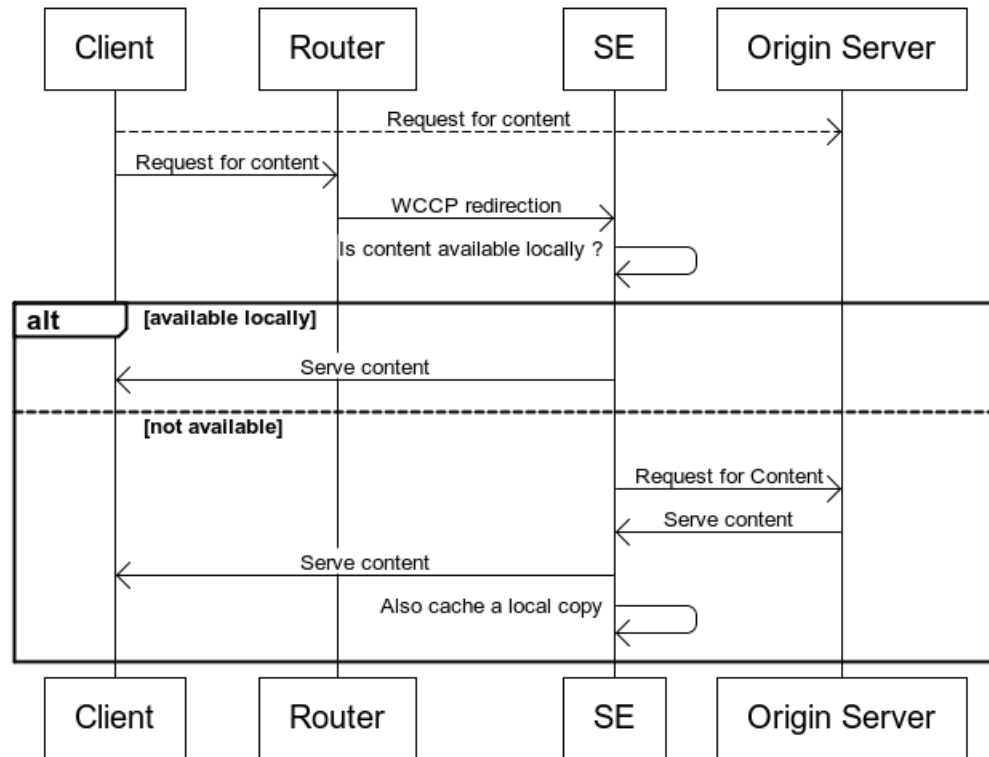
Table 2-1 *Delivery Service Parameters Example*

Parameter	Value
Type	Caching/Prefetch
Origin Server	www.ivs-example.com
Service Routing Domain Name	cr-ivs.example.com
Delivery Service Contents	http://www.ivs-example.com/video/wmv-152 http://www.ivs-example.com/video/wmv-92 http://www.ivs-example.com/video/wmv-212 http://www.ivs-example.com/video/wmv-59 type= “cache” http://www.ivs.example.com/video/wmv-6 type= “cache”

Content Request Using WCCP

Figure 2-4 describes the typical WCCP content workflow.

Figure 2-4 WCCP Workflow



WCCP Services

WCCP configuration settings for the Service Engine are managed with the CDSM graphical user interface (GUI) beginning in ECDS Release 2.5.5. Access SE request routing administration by choosing:

Devices > Request Routing > WCCP

See the following sections for information about WCCP services:

- [WCCP Service Negotiation, page 2-16](#)
- [WCCP Service Groups, page 2-16](#)
- [Dynamic WCCP Redirection Services, page 2-17](#)
- [WCCP Custom Web Cache Service, page 2-17](#)

WCCP Service Negotiation

The Administrator creates a WCCP service on the cache engine (Streaming Engine, or SE) and assigns a router to the created service. The SE sends a “HERE_I_AM” message to the router. The router replies with the “I_SEE_YOU” message. Each of the messages contain enough information for the routers and the service engines to be aware of the router list, service engine list, service IDs, and so on.

**Note**

These messages are also a form of KeepALive message. If the continuous message stream is lost for an amount of time longer than the preset threshold, the service is automatically removed from the service group.

WCCP Service Groups

WCCP uses the concept of a service group to define caching related services for a WCCP-enabled router and WCCP-enabled Service Engines in a cluster. Service groups are identified by a service group number. Each WCCP service group number specifies a router list, single port list (containing up to eight ports), application type, hash parameters, password, and weight (for load balancing).

[Table 2-2](#) lists the service group numbers and describes the services supported by a WCCP-enabled router. For more information, see [Table 7-2](#) in the “[Configuring WCCP General Settings](#)” section on page 7-1.

Table 2-2 **WCCP Service Groups**

Service Group Number	Description of Services
0	WebCache
70	HTTPS
80	RTSP
81	MMS
84	RTMP
90–97	Dynamic Service (user-configurable)
98	Custom Web-Cache

A WCCP-enabled Service Engine supports various Internet protocols depending on the style of the request URL. If the WCCP-enabled Service Engine receives a server-style URL, only HTTP(S) and RTSP protocols are supported (if the RTSP user agent criteria is met). If the WCCP-enabled Service Engine receives a proxy-style URL, the HTTP(S) and RTSP protocols are supported, as long as the respective proxy services are configured on the Service Engine. Proxy-style request URLs include the protocol and host name, whereas server-style request URLs do not. The RTSP protocol is supported for both server-style and proxy-style requests.

For proxy-style requests, the Service Engine supports up to eight incoming ports each for HTTP, MMS, and RTSP proxy modes. The incoming proxy ports can be the same ports that are used by transparent mode services. The incoming proxy ports can be changed without stopping any WCCP services running on the Service Engine or on other Service Engines in the Service Engine farm.

The Service Engine WCCP implementation currently allows global settings that apply to all WCCP services, such as healing parameters, slow start, and others. The multiple service model does not change that, and the settings in question remain global for the whole WCCP system. (See the [“Configuring WCCP General Settings” section on page 7-1.](#))

Dynamic WCCP Redirection Services

You can configure the Service Engines to handle up to eight user-configurable or dynamic WCCP redirection services (service group numbers 90 to 97) on a Service Engine, provided that the services are also configured on the router.

With 8 dynamic services using a maximum number of 8 ports each, the maximum number of ports that can be specified for transparent redirection is 64.

WCCP Custom Web Cache Service

Custom web cache service (service number 98) causes the Service Engine to establish WCCP Version 2 redirection services automatically with a Cisco router on a user-specified port number. The Service Engine then performs transparent web caching for all HTTP requests over that port while port 80 transparent web caching continues without interruption. For custom web caching, service 98 must be enabled on the routers.

Transparent caching on ports other than port 80 can be performed by the Service Engine when WCCP is not enabled or when client browsers have previously been configured to use a legacy proxy server. The following features combine to support WCCP transparent caching:

- [WCCP Interception, page 2-17](#)
- [WCCP Redirection, page 2-18](#)
- [WCCP Load Balancing- Source and Destination IP Hash, page 2-18](#)
- [WCCP Availability Monitoring, page 2-19](#)
- [WCCP Failover, page 2-19](#)
- [Multiple Router/Multiple Service Engine Support, page 2-19](#)
- [Additional WCCP Support, page 2-19](#)

WCCP Interception

The service group servers monitor interfaces based on interception configuration criteria to identify traffic to be redirected to a service group client:

- Ingress redirection (inbound): When applied to an interface, the router monitors traffic entering an interface to see if it matches criteria for any of the running service groups.
- Egress redirection (outbound): When applied to an interface, the router monitors traffic leaving an interface to see if it matches criteria for any of the running service groups.

WCCP Redirection

WCCP Version 2 tells the network which packets to redirect to the SE. Service group servers (routers) can use one of two methods to redirect traffic to an SE:

- GRE—This is the most commonly use method. The entire packet is encapsulated into a new IP packet that is destined for the SE.
- Layer 2 redirect—Less frequently used, but common with LAN switches. The original frame header is rewritten with the SE MAC address as destination and then forwarded to the SE.

WCCP Load Balancing- Source and Destination IP Hash

Routers and cache engines become aware of each other and form a service group using the WCCP management protocol. Once the service group has been established, one of the cache engines is designated to determine load assignments among the cache engines.

If there is a group of cache engines, the one seen by all routers and that has the lowest IP address becomes the lead cache engine. The role of this cache engine is to determine how traffic should be split across cache engines. The assignment information is passed to the entire service group from the designated cache engine so that the routers of the group can redirect the packets properly and the cache engines of the group can manage their load better.

WCCP Version 2 allows for load balancing based on a number of parameters, including source information (IP address, subnet, port) or destination information (IP address, subnet, port).

With the hash assignment method, the hash parameters specify how traffic should be load balanced among the different service groups. Specifically, hashing maps items from one item set to another, such as mapping destination IP addresses or destination ports to different Service Engines in a service group from the WCCP-enabled router for load-balancing purposes. Only one load-balancing method can be used per Service Engine farm.

See the following sections for more information about load balancing:

- [Hash Assignment, page 2-18](#)
- [Mask Assignment, page 2-19](#)
- [Weight Assignment, page 2-19](#)

For more information, see the “[Load Balancing Command Examples](#)” section on [page 7-22](#).

Hash Assignment

The default assignment method, hash assignment, uses a 256-bucket redirection hash table to distribute traffic across the WCCP clients in a service group. As a WCCP server intercepts traffic, the source/destination IP address or source/destination port (depending on the service group configuration) is run through a hash function to produce an index value. The index value maps into one of the 256 buckets in the hash table. Each bucket in the hash table is assigned to a WCCP client in the service group.

**Note**

Web-cache service does not get a hash assignment.

For more information, see the “[Hash Assignment Command Example](#)” section on [page 7-23](#).

Mask Assignment

Mask assignment uses masks and a table of values to distribute traffic across the WCCP clients in a service group. Mask assignment was developed specifically for the Cisco Catalyst series switches, and is one of the key characteristics that enables WCCP interception to be performed completely in hardware on these platforms. As the WCCP server intercepts traffic, a bitwise AND operation is performed between each mask value and the contents of the packet (specifically the source/destination IP addresses and ports). The result is then compared to a list of values for each mask. Each value is assigned to a specific WCCP client in the service group. The following figure shows the masking and value assignment concept.

Weight Assignment

Weight assignment is used when one SE is determined to have better hardware performance than another and you would like to shed more buckets to the better performing SE. Once the buckets have been shed to the better performing SE, the router redirects the traffic as usual using the appropriate assignment method.

For more information, see the [“Weight Assignment Command Example” section on page 7-24](#).

WCCP Availability Monitoring

WCCP Version 2 keepalive (heartbeat) information is exchanged every 10 seconds between SEs and the router. If an SE is unresponsive for three consecutive heartbeats, it is removed from the service group.

WCCP Version 2 heartbeat uses UDP port 2048.

WCCP Failover

If a SE within a service group fails, the portion of the load that it was handling is automatically distributed to other SE within the service group. If no additional SEs are available, the service group is taken offline and packets are not redirected.

Multiple Router/Multiple Service Engine Support

With WCCP Version 2, multiple routers can service a cluster, creating contention between available routers to obtain status as the device that redirects packets for data coming from each of the cache engines in the cluster. A maximum of 32 routers together with 32 Service Engines are supported in any one WCCP Service Group, which increases the service capability and adds greater bandwidth. For configuration information, see the [“Managing WCCP Router Lists” section on page 7-12](#).

WCCP single Service Engine deployment is also supported; one SE and one router can be deployed in the WCCP network.

Additional WCCP Support

The following features introduced for the Cisco ECDS with WCCP are listed alphabetically:

- [TCP Flow Protection, page 2-20](#)

- [Slow Start, page 2-21](#)
- [WCCP Service Negotiation, page 2-16](#)
- [Dynamic Service and Port List, page 2-21](#)
- [WCCP Transparent Routing Bypass Options, page 2-21](#)

TCP Flow Protection

TCP flows are protected when a Service Engine is added to or removed from a service group. Because all buckets are re-allocated, there is a chance that some buckets might be assigned to the new Service Engine when a new service engine is added to the service group. In that case, TCP traffic belonging to that bucket will be broken. Flow protection is a mechanism on the new service engine to forward that broken TCP flow back to its original service engine, keeping TCP flow intact.

WCCP TCP flow protection is managed by the **wccp flow-redirect enable** command. See the [“Load Balancing Command Examples” section on page 7-22](#) for configuration information.

The following sections describe how TCP flow is managed:

- [Graceful \(Clean\) Shutdown, page 2-20](#)
- [Flow Redirection, page 2-20](#)

Graceful (Clean) Shutdown

To prevent broken TCP connections after a reload, version change or enabling or disabling WCCP, the Service Engine performs a clean shutdown before you begin the reload. The Service Engine does not reboot until all connections have been serviced or the configured maximum wait interval has elapsed.

During a clean shutdown, the Service Engine continues to service the flows it is handling but starts to bypass new flows. When the number of flows goes down to zero, the Service Engine takes itself out of the cluster by having its buckets reassigned to other Service Engines by the lead Service Engine. TCP connections can still be broken if the Service Engine crashes or is rebooted without WCCP being cleanly shut down. The clean shutdown can be aborted while in progress.



Tip

You must first configure WCCP General Settings before you can use this feature. See the [“Configuring WCCP General Settings” section on page 7-1](#).

Graceful shutdown is managed by the **no wccp version 2** command. For more information, see the [“Load Balancing Command Examples” section on page 7-22](#).

Flow Redirection

In some cases you may want to bring an SE online or remove it from a service group to ensure that no existing flows are broken. This action:

- Allows preexisting TCP flows to continue.
- Allows existing flows serviced by preexisting SEs in the cluster continue to receive flows when an SE is added to the group.

Flow redirection is managed by the **wccp flow-redirect** command. See the [“Load Balancing Command Examples” section on page 7-22](#) for configuration information.

Slow Start

Within a cluster of Service Engines, TCP connections are redirected to other Service Engines as units are added or removed. A Service Engine can be overloaded if it is reassigned new traffic too quickly or if it is introduced abruptly into a fat pipe. To prevent a Service Engine from being overwhelmed when it comes online or is reassigned new traffic, enable the slow start provides the following:

- TCP flow protection when WCCP Version 2 is enabled and a Service Engine is introduced into the cluster.
- TCP flow protection when WCCP Version 2 is disabled and a Service Engine is leaving the cluster.
- Load assignment to the Service Engine in slow increments rather than a full load at boot up.

Slow start is applicable only in the following situations:

- During initial boot up when there is no Service Engine present in the server farm.
- When a new Service Engine is added to a cluster that is not handling the full load; for example, when there are some buckets that are being shed by the cluster.

In all other cases slow start is not necessary and all the Service Engines can be assigned their share of traffic right away. Slow start is managed by the **wccp slow-start** command. See the [“Configuring WCCP General Settings” section on page 7-1](#) and the [“SE\(config\)# wccp slow-start enable” section on page 7-22](#) for more information.

Dynamic Service and Port List

Dynamic service in WCCP provides wider port choices for more applications. The typical setup involves the non-standard port of applications running on the origin server, but you can use any port. The setup works as follows:

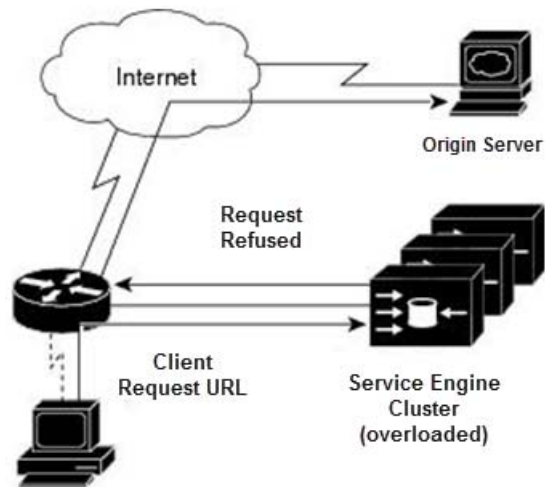
1. The administrator uses the dynamic service number provided on the WCCP configuration to associate with a port-list number.
2. The service engine uses the configured dynamic service number to allow WCCP service.
3. The WCCP router treats the dynamic service as usual and redirects the packet.

WCCP Transparent Routing Bypass Options

One of the fundamental principles of transparent network request redirection is that the Service Engine must remain transparent to the end user at all times. A transparent caching solution in a network environment must not introduce any possible failure conditions or side effects in the network.

The Cisco ECDS transparent caching solution uses a WCCP-enabled router and various advanced techniques to ensure that the Service Engine remains transparent, even if web browsers are nonoperational or web servers are not HTTP-compliant.

If a Service Engine becomes overwhelmed with traffic, it can use the overload bypass feature to reroute the overload traffic. When the Service Engine is overloaded and the **bypass load** command is enabled, the Service Engine refuses additional requests and forwards them to the origin servers. If the load remains too high, more traffic is bypassed to the servers, and so on until the Service Engine can handle the load. The time interval between one bucket being bypassed and the next is set by the **out-interval** option. The default is 4 seconds. See

Figure 2-5 Overload Bypass

When the first bucket bypass occurs, a set interval must elapse before the Service Engine begins to resume service to the bypassed buckets. When the Service Engine begins to serve bypassed traffic again, it means that the overload timer has timed out. Once bypass load is enabled, whenever the system CPU and memory usage has exceeded its threshold, bypass is triggered. The Service Engine stops the bypass process and begins service again when the configured time interval has been reached. Time interval default is 5 minutes.

Bypass and time interval are managed by the following commands:

```
bypass load enable
bypass load time-interval 5 (minutes)
```

See the [“Configuring WCCP Transparent Routing Bypass Settings”](#) section on page 7-18 for more information.

HTTP and HTTPS Support

See the following sections for HTTP and HTTPS support with ECDS:

- [Web Engine HTTP Connections, page 2-22](#)
- [IP Spoofing for HTTP, page 2-23](#)
- [HTTPS Caching, page 2-24](#)

Web Engine HTTP Connections

To access HTTP Connections in the ECDS GUI, choose **Devices > Application Control > Web > HTTP > HTTP Connections**. For more information, see the [“Configuring Web Engine HTTP Connections”](#) section on page 5-39.

The Outgoing HTTP Proxy Bypass Domains option in the ECDS GUI allows a Service Engine to skip some connections based on source and destination IP addresses. The SE will not forward packets being sent to these domains to the Outgoing Proxy. This feature is activated when you select the Enable Outgoing Proxy check box. You can create an outgoing proxy bypass list with up to 32 space-separated entries.

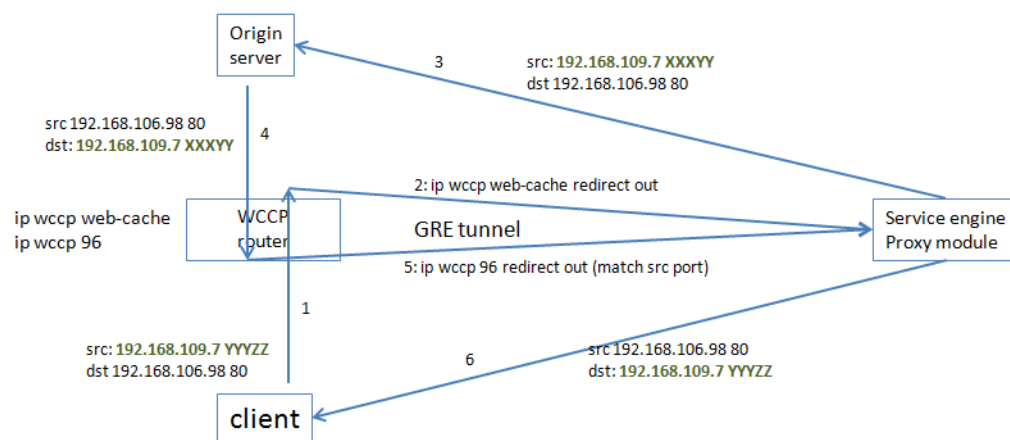
For more information, see [“Configuring the Outgoing Proxy Bypass List” section on page 5-42](#).

IP Spoofing for HTTP

IP Spoofing enabled on a WCCP v2 router allows the Service Engine to send and receive packets with the client IP (which is different from the Service Engine IP address), and then sends the packets to the waiting application. The router intercepts the packets from both the client and the server transparently, and forwards these redirected packets to the same Service Engine so that the TCP connection is not broken.

With typical transparent caching, an end user issues an HTTP request from a web browser. This request is transparently intercepted and sent to the Service Engine (acting as a transparent proxy server) by a WCCP router (Figure 2-6).

Figure 2-6 IP Spoofing Intercept and Redirect



The Service Engine accepts the incoming TCP connection from the WCCP router, determines that the request is for an object not in storage (cache miss), and issues a request to the origin server for the requested object. When the Service Engine contacts the origin server, it uses its own IP address instead of the client IP address for which it is making the request.

If IP spoofing is configured on the WCCP Version 2-enabled routers and the Service Engines, the Service Engine (acting as a transparent proxy server) can send out the client's IP address to the origin server for authentication purposes instead of sending out the request with its own IP address. The WCCP router intercepts packets from the server that are destined for the client's IP address, and redirect these packets to the Service Engine to maintain TCP flow integrity.

By spoofing a client's IP address, the following capabilities are supported:

- The Service Engine can send out packets with the client IP (which is different from the Service Engine's own IP address).

- The Service Engine can receive packets with the client IP (which is again different from the Service Engine's own IP address), and send the packet to the correct application that is waiting for the packet.
- The WCCP Version 2-enabled router can intercept the packets from both the client and the server transparently, and forward these redirected packets to the same Service Engine so that the TCP connection is not broken.

When configured for IP spoofing, the Service Engine connects to the origin server using the client IP address instead of its own IP address. At this point, the router cannot identify requests coming from the Service Engine because the source IP address of the request is not that of Service Engine.

**Caution**

IP Spoofing is available only when WCCP is enabled.

1. See the [“Configuring WCCP General Settings” section on page 7-1](#) to enable WCCP in the ECDS GUI.
2. See the [“Configuring HTTP IP Spoofing with WCCP” section on page 7-19](#) to enable IP Spoofing in the ECDS GUI

HTTPS Caching

WCCP Version 2 supports transparent HTTPS redirection for ECDS deployments. Access Service Engine HTTPS administration by choosing:

Devices > Application Control > Web > HTTPS

The following are general features that support HTTPS caching:

- [Transparent HTTPS Caching Using SSL, page 2-24](#)
- [HTTPS Certificates, page 2-25](#)
- [HTTPS Service Rules, page 2-25](#)
- [HTTPS Requests on Ports, page 2-25](#)
- [HTTPS Connection Statistics, page 2-25](#)
- [HTTPS Protocol Protection, page 2-26](#)

Transparent HTTPS Caching Using SSL

Transparent HTTPS caching using SSL works as follows:

1. The Service Engine, configured as an HTTPS server, receives an HTTPS request redirected through a WCCP-enabled router.
2. The Service Engine sends back an SSL certificate (obtained from the origin server) to the requesting client to negotiate an SSL connection.
3. The client sends HTTPS requests inside the negotiated SSL connection.
4. The Service Engine examines the request, looks in its cache, and performs normal HTTP request processing.
5. If the Service Engine can fulfill the request from its local storage (cache hit), it sends the requested content back using the SSL connection.

6. If the Service Engine cannot fulfill the request from its local storage (cache miss), it initiates a connection to the origin server to retrieve the requested content through the SSL connection.
7. The Service Engine caches the requested content (if possible) and also sends a copy to the requesting client through the negotiated SSL connection.

For the SSL-termination feature to work properly, you must install the SSL certificate and private key of the origin HTTPS servers on the Service Engine. The SSL-termination feature works in transparent mode if the Service Engine has the correct certificates and private keys installed. For specific requested content to be cached, you must import the proper certificates and keys for these origin HTTPS servers into the Service Engine and configure the Service Engine to cache content from these origin HTTPS servers. See the [“Configuring HTTPS Certificates” section on page 5-49](#) for more information.

HTTPS Certificates

HTTPS prepositioned caching and HTTPS dynamically cached content is supported through self-signed certificates with keys that are generated outside the Service Engine and imported to the SE.

A digital certificate is a credential that allows the Service Engine to be presented to an HTTPS client as the origin HTTPS server, enabling encrypted communication and secure identification of a network webserver.

The Service Engine accepts certificates in Privacy-Enhanced Mail (PEM) format, which is used by Apache servers. The Service Engine uses PEM format internally, and automatically converts certificates in PKCS #12 format to PEM format. If you need to use a certificate in a different format, first convert it to one of these supported formats.

See the [“Configuring HTTPS” section on page 5-48](#).

HTTPS Service Rules

You can specify a set of rules using the Rules Template licensed feature for HTTPS; Service Rule functions that apply to HTTP also apply to HTTPS. See the [“Configuring Service Rules” section on page 5-11](#).

HTTPS Requests on Ports

The Service Engine provides configurable options to receive HTTPS requests on ports other than 443, which is the default. See the [“Configuring HTTPS” section on page 5-48](#).

HTTPS Connection Statistics

New CLI commands and CDSM statistics tools are available to monitor connections per domain.

- WCCP status **show** command:

```
show wccp
```

- Updated logging retrieval—Access logs by entering the following on the SE:

```
cd local/local1/service_logs
```

HTTPS Protocol Protection

The Service Engine provides an option to reject access to file objects if requesting protocol is anything other than HTTPS

Transparent Proxy Support for HTTPS (Live and VoD)

The Service Engine provides an option to receive HTTPS requests as a proxy and send requests to the HTTPS origin via separate outgoing proxy for dynamic caching. See [Appendix F, “Configuring Primary and Backup Proxy Servers.”](#)

Programs

A Cisco ECDS program is a scheduled live or rebroadcast event that streams content to client devices. The ECDS streams live or rebroadcast content by using the Movie Streamer, Windows Media Streaming, or Flash Media Streaming Engine.

Movie Streamer live and rebroadcast programs can have multiple tracks (1–3 tracks).

See the following sections for supported programs:

- [Live Programs, page 2-27](#)
- [Rebroadcasts, page 2-27](#)
- [API Program File, page 2-27](#)

Live Programs

Live events are streamed from third-party encoders (such as Windows Media Encoder Version 9 or the QuickTime encoder) or from streaming servers (such as Windows Media Server). The live stream is ingested by the Content Acquirer and transmitted to all Service Engines using either unicast or multicast. The live stream is transmitted to end users by using either multicast or multicast/unicast live splitting. The live stream is only available to end users during its scheduled times.

With live stream splitting, administrators do not have to create scheduled multicast events, because the Service Engines automatically split the stream.

Unicast to multicast streaming is a solution similar to live stream splitting, except that in the final delivery segment the stream is converted to multicast to minimize the bandwidth demand on the ECDS network and to minimize the load on the Service Engines.

Each live program can have up to ten different playtimes scheduled. The program is broadcast from all Service Engines simultaneously.

Rebroadcasts

In a scheduled rebroadcast, prefetched content is scheduled to be streamed from the Service Engines using multicast. Content can only be selected from one delivery service. The Service Engines and device groups assigned to the delivery service are automatically selected when the content files are chosen for the program.

API Program File

Programs can be defined through the Enterprise CDSM or through an API. Programs created through APIs are based on a program file. A program file is an XML file that resides on an external server and contains the elements that define the schedule, content, and presentation parameters. The Enterprise CDSM gets the program file, parses it, and saves the program file to the database. The program is automatically updated at intervals by refetching the program file and reparsing it. RTSP is the only protocol supported in the program file.

Programs created using an API can be viewed in the Enterprise CDSM as read-only, and modifications to the API programs can be accomplished through the API. The API program can also be edited using the Enterprise CDSM; however, the information about the API program file is deleted and the program can no longer be modified through the API. A third option is to copy the API program using the Copy Program feature.

Where to Go Next

Proceed to [Chapter 3, “Getting Started”](#) to learn about initial device configuration, logging into and navigating the Cisco ECDS, and to see n examples of a typical ECDS configuration workflow.

**Tip**

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Configuration Guide on Cisco.com.



CHAPTER 3

Getting Started

The following sections describe initial device configuration, logging into and navigating the Enterprise Content Delivery System Manager (Enterprise CDSM), and provides an example of a typical ECDS configuration workflow:

- [Configuring the Cisco Media Delivery Engines for the First Time, page 3-1](#)
- [Logging In to the Enterprise CDSM, page 3-1](#)
- [Activating and Synchronizing the Devices, page 3-3](#)
- [Navigating the Enterprise CDSM, page 3-6](#)
- [Configuring Primary and Standby Enterprise CDSMs, page 3-11](#)
- [Typical Configuration Workflow, page 3-14](#)
- [Where to Go Next, page 3-15](#)

Configuring the Cisco Media Delivery Engines for the First Time

You must initially configure the Media Delivery Engines (MDEs) before they can participate in the ECDS network. The MDE that runs the Enterprise CDSM must be initialized first so that the MDEs running the Service Engine (SE) and Service Router (SR) can register with it.

1. Go to the [Cisco Enterprise Content Delivery System Quick Start Guide](#) for instructions to initially configure the MDEs.
2. After you have initially configured your MDEs, you must activate the SEs and SRs and configure the internal clocks by using the Enterprise CDSM:
 - a. First log into the Enterprise CDSM ([Logging In to the Enterprise CDSM](#)).
 - b. Then see the “[Activating and Synchronizing the Devices](#)” section on [page 3-3](#).

Logging In to the Enterprise CDSM

To log in to the Enterprise CDSM:

-
- Step 1** Using your web browser, enter the IP address of your Enterprise CDSM and port number **8443**. For example, if the IP address of your Enterprise CDSM is 192.168.0.236, enter:
`https://192.168.0.236:8443`

The Security Alert message is displayed.



Tip

If you are using Mozilla Firefox version 3.01 or higher as your web browser, you need to add the Enterprise CDSM IP address to the exception list. After entering the Enterprise CDSM IP address with port **8443**, Firefox displays a Secure Connection Failed message with a link stating “Or you can add an exception.”

a. Click this link, then click **Add Exception**. The Add Security Exception dialog box is displayed.

b. Click **Get Certificate**, and then click **Confirm Security Exception**.

The Enterprise CDSM IP address has been added to the exception list and you no longer get the Secure Connection Failed message.



Note

Sometimes the Enterprise CDSM is not initially accessible from a web browser. If this occurs you must disable and re-enable the Centralized Management System (CMS). Log in to the CLI for the Enterprise CDSM, and enter the global configuration command **no cms enable** followed by **cms enable**.

Step 2 Click **Yes** to accept the security certificate. The Login page is displayed (Figure 3-1).

Figure 3-1 The Enterprise CDSM Login Page



Step 3 Enter your username and password and click **Login**. The Enterprise CDSM home page is displayed. The built-in username is *admin* and the initial password is *default*.



Note

We strongly recommend that you change the built-in admin password as soon as possible. To do so, log in to the CLI of the Enterprise CDSM device, and use the **username admin password <password>** global configuration command.

**Note**

If the default username and password have been changed by another Enterprise CDSM administrator, you need to get the new username and password.

Activating and Synchronizing the Devices

The ECDS administrator approves a device by making it active. This security feature prevents unauthorized devices from joining the ECDS.

**Caution**

All devices must be synchronized with each other for the ECDS to function properly.

Synchronization ensures accurate timestamps in all the logs and accuracy in caching decisions determined by If Modified Since (IMS) lookups. Using Network Time Protocol (NTP) to synchronize the devices in the ECDS is the best practice.

**Note**

If the network is not configured with NTP, then every device in the ECDS must be configured with exactly the same time and time zone. We recommend that you use an NTP server for network synchronization.

Activating and Setting NTP for Each Device

**Tip**

To navigate within the Enterprise CDSM, click one of the tabs (for example, **Devices**) and then one of the tab options (for example **Locations**). Navigational directions in procedures are written in the following way:

Devices > Devices > Assignments > Device Groups

**Note**

From the Devices Table, you can activate all inactive devices by clicking the **Activate All Inactive SEs** icon. See the [“Activating All Inactive Service Engines”](#) section on page 3-5.

To activate and synchronize a Service Engine (SE) or Service Router (SR):

Step 1

From the Enterprise CDSM home page, choose **Devices > Devices**. The Devices Table is displayed ([Figure 3-2](#)) listing all the registered SEs and SRs.

Figure 3-2 *Devices Table Page—Edit Device*

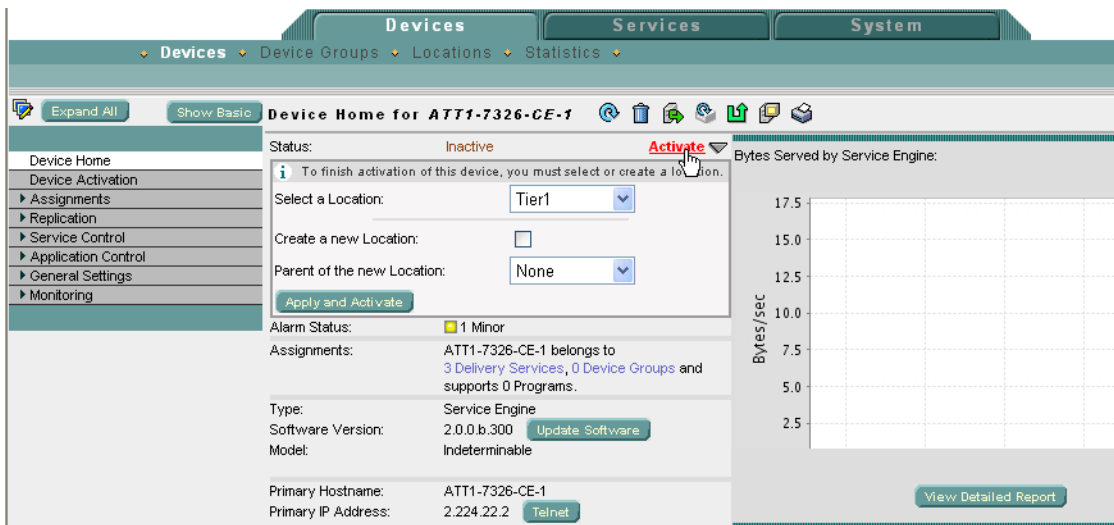

Device Name	Type	IP Address	Status	Location	Software Version
Edit NE-CDM-612-9	Content Delivery System Manager (Primary)	3.1.4.18	Online		2.0.0.b.430
NE-612-12	Service Engine	3.1.4.31	Online	NE-612-12-location	2.0.0.b.410
Q5-CDE200-2	Service Engine	2.225.2.56	Online	Q5-CDE200-2-location	2.0.0.b.420

Step 2 Click the **Edit** icon next to the device name. The Devices home page is displayed.

If the device you want to activate is not listed in the Devices Table, restart the CMS for that device by telnetting to it and performing the following actions:

- Enter **no cms enable** in global configuration mode.
- Enter **cms deregister force** at the user prompt to disassociate with the prior registered CDSM.
- Enter **cms enable** in global configuration mode to restart service.

Step 3 Click **Activate** in the Devices home page. The Location dialog box is displayed (Figure 3-3).

Figure 3-3 *Devices Home Page—Location Dialog Box*


Device Home for ATT1-7326-CE-1

Status: Inactive **Activate**

To finish activation of this device, you must select or create a location.

Select a Location: Tier1

Create a new Location: ☐

Parent of the new Location: None

Apply and Activate

Alarm Status: 1 Minor

Assignments: ATT1-7326-CE-1 belongs to 3 Delivery Services, 0 Device Groups and supports 0 Programs.

Type: Service Engine

Software Version: 2.0.0.b.300 **Update Software**

Model: Indeterminable

Primary Hostname: ATT1-7326-CE-1

Primary IP Address: 2.224.22.2 **Telnet**

Bytes Served by Service Engine:

View Detailed Report

Step 4 Create or choose a location. To activate an SE, you need to assign it to a location.

Because the standby Enterprise CDSM is global to the ECDS network, it does not need to be assigned to a location.

You have the following options in creating or choosing a location:

- If you have already created locations, you can choose a location from the **Location** drop-down list.
- To create a default location, which can be edited later, check the **Create a New location** check box. A default location is created with the following name: **<SE-name>-location**. From the **Parent of the New Location** drop-down list, choose a parent for this location.

For information about creating locations, see the “[Configuring Locations](#)” section on page 4-1.

Step 5 Click **Apply and Activate**.

The Status of the device shows “pending” until the device is fully activated. This may take a few minutes.

- Step 6** To display the top-level Table of Contents, click the **Show All** button above the Contents pane.
- Step 7** From the left-panel menu, select **General Settings > Network > NTP**. The NTP Settings page is displayed.
- Step 8** Check the **Enable** check box and enter the IP address or hostname of each NTP server. Use a space to separate each server.
- Step 9** Click **Submit** to save your settings.
- The activation and NTP server settings must be completed for each SE, SR, and standby Enterprise CDSM.



Tip

For a quick way to get to other SEs, click the **Display All Devices** icon located to the left of the Expand All button. This icon toggles between the Display All Devices and Menu icons.

For more detailed information about configuring locations, activating devices, and configuring NTP servers, see the following sections:

- [Configuring Locations, page 4-1](#)
- [Activating a Service Engine, page 5-1](#)
- [Configuring NTP, page 5-79](#)

Activating All Inactive Service Engines

To activate all inactive SEs:

- Step 1** From the Enterprise CDSM home page, choose **Device > Devices** and click the **Activate All Inactive SEs** icon. See [Figure 3-4](#).

Figure 3-4 *Devices Table Page—Activate All Inactive Service Engines*

Devices						
Devices Device Groups Locations Statistics						
Devices  Activate all inactive SEs Rows: 10						
Device Name	Type	IP Address	Status	Location	Software Version	
NE-612-12	Service Engine	3.1.4.31	Online	NE-612-12-location	2.0.0.b.410	
NE-612-5	Service Engine	3.1.4.14	Online	tier-1	2.0.0.b.400	
NE-612-6	Service Engine	3.1.4.15	Online	tier-2	2.0.0.b.430	

The Location Choice page is displayed ([Figure 3-5](#)).

Figure 3-5 **Location Choice Page**

Step 2 In the Location Choice page, click either **Select an Existing Location for All Inactive SEs** or **Create a New Location for Each Inactive SE**.

If you are creating a new location, you can select a parent location, or leave the default of “none.”

Step 3 Click **Submit** to save the settings.

The Status in the Devices Table for all the inactive SEs shows “pending” until the devices have been fully activated.

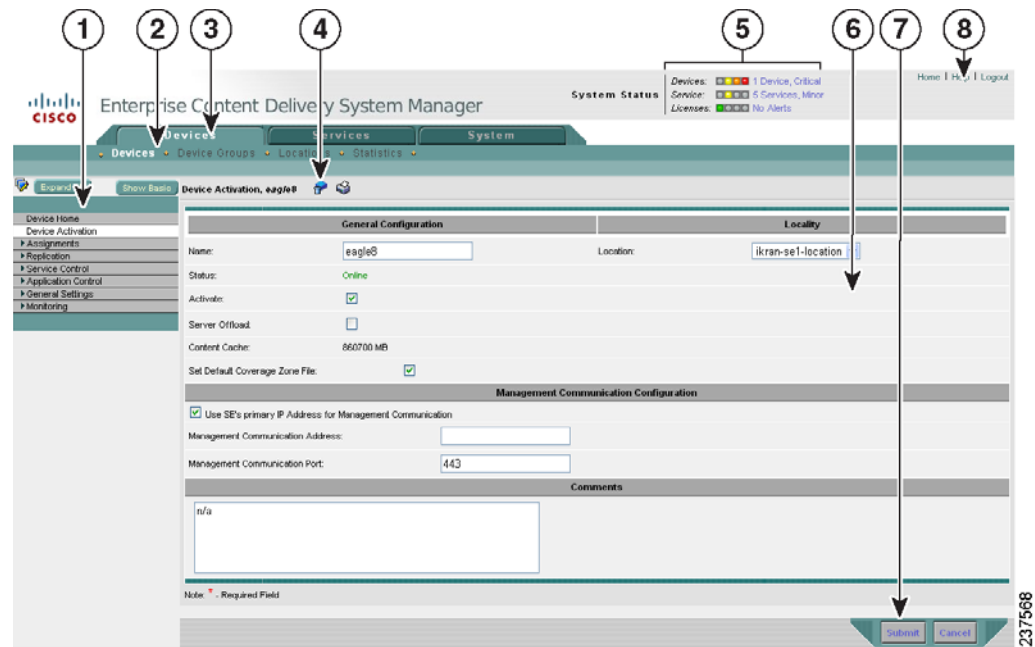


Note

All devices activated in this way need to have the NTP settings configured. See [Step 6](#) through [Step 9](#) in the “[Activating and Setting NTP for Each Device](#)” section on page 3-3.

Navigating the Enterprise CDSM

[Figure 3-6](#) shows the different elements of the Enterprise CDSM.

Figure 3-6 Enterprise CDSM User Interface

1	Left panel menu	5	System Status bar
2	Tab options	6	Page
3	Tabs	7	Submit and Cancel buttons
4	Task bar	8	Tools (Home, Help, and Logout)

The System Status bar, tabs, tab options, and tools are accessible from any page in the Enterprise CDSM. The left panel menu changes depending on which tab and tab option you choose.

Devices, Services, and Other Tables

The Devices Table page shows all the devices registered in the Enterprise CDSM. [Figure 3-7](#) shows an example of the Devices Table page. A table is displayed for each of the following tab options:

- Devices (from Devices tab)
- Device Groups (from Devices tab)
- Locations (from Devices tab)
- Delivery Services (from Services tab)
- Live Video (from Services tab)

Figure 3-7 Devices Table Page

Device Name	Type	IP Address	Status	Location	Software Version
NE-612-12	Service Engine	3.1.4.31	Online	NE-612-12-location	2.0.0.b.450
NE-612-5	Service Engine	3.1.4.14	Online	tier-1	2.0.0.b.470
NE-612-6	Service Engine	3.1.4.15	Online	NE-612-12-location	2.0.0.b.470
NE-612-7	Service Engine	3.1.4.16	Online	tier-1	2.0.0.b.470
NE-7326-2	Service Engine	3.1.4.21	Online	tier-3	2.0.0.b.470
NE-CDM-612-9	Content Delivery System Manager (Primary)	3.1.4.18	Online		2.0.0.b.470
NE-CR-612-4	Service Router	3.1.4.13	Online	tier-1	2.0.0.b.470
Q5-CDE200-1	Service Engine	2.225.2.11	Offline	tier-1	2.0.0.b.410
Q5-CDE200-2	Service Engine	2.225.2.56	Offline	Q5-CDE200-2-location	2.0.0.b.420
Q5-CDE200-4	Service Engine	2.225.2.14	Online	tier-1	2.0.0.b.440

You can sort the information in the table by clicking on any column title. The table can be sorted in ascending or descending order for each column. The task bar options provide other table manipulations, including filtering, refreshing the table, viewing all items, and printing.

The bottom of the table lists the page number and the total number of pages, as well as how many items are showing out of the total number of items.

The table defaults to listing ten rows. You can change the number of rows shown by clicking the Rows drop-down list.

To get more information on an item or to configure an item, click the **Edit** icon to the left of the item name. To create a new item, click the **Create New** icon in the task bar.

Devices Home Page

The Devices home page provides information about the device, as well as the ability to perform the following tasks:

- Activate the device
- Telnet to the device (Telnet is disabled by default.)
- Update the device software
- Assign the device to baseline groups

From the Devices home page you can access the delivery services and device groups the device is assigned to, by clicking the appropriate link. All delivery services, or device groups (depending on which link you clicked), configured in your ECDS are displayed. Through this page, you can assign the device to additional delivery services or device groups by clicking the icon next to the applicable delivery services or device groups and submitting your selection.

The Devices home page offers detailed bandwidth and bytes-served graphs with detailed reports for each.

The left panel menu has two toggle buttons: Show Basic/Show All and Expand All/Collapse All.

- **Show All** Shows all the menu items in the menu.
- **Show Basic** Shows only the Device home menu item.

- **Expand All** Shows every menu and submenu.
- **Collapse All** Shows only the top-level menu items.

Task Bar

The task bar displays information about the page you are on and provides associated tasks. All task bar icons, as well as other icons, have labels that are displayed when you roll over the icon with your mouse pointer.

Any icon used in a procedure is referenced by the rollover label; for example, **Create New** is the rollover label for the following icon:



Table 3-1 describes the icons available in the Enterprise CDSM.

Table 3-1 Enterprise CDSM Icons

Icon	Function
	Activates all inactive Service Engines.
	Displays devices.
	Displays left-panel menu.
	Deactivates the device.
	Updates application statistics.
	Forces refresh of replication information or process content changes.
	Goes back to Replication Status page.
	Forces full database update.
	Forces settings on SEs in group.
	Forces the group settings.
	Views read-only items.

Table 3-1 *Enterprise CDSM Icons (continued)*

Icon	Function
	Creates a new item.
	Edits an item.
	Deletes an item.
	Adds a content item for acquisition.
	Deletes a selected item.
	Manages between host and proxy servers for content acquisition.
	Saves to disk.
	Views complete URL (+) or view (-) partial URL that is used to acquire content.
	Exports a table to a comma-separated value (CSV) file.
	Creates a filtered table. Filter the table based on the field values.
	Displays a graph.
	Applies the default settings to the device.
	Overrides the group settings on the device.
	Views all table entries. Click this icon to view all entries after you have created a filtered table.
	Refreshes the table.
	Reboots the device.
	Prints the current window.
	Copies a program.
	Previews a program.

Table 3-1 Enterprise CDSM Icons (continued)

Icon	Function
	Assigns all items to the entity.
	Removes all items from the entity.
	Indicates that the current transaction was successfully completed.
	Indicates that user input is invalid and that the transaction did not finish.

Configuring Primary and Standby Enterprise CDSMs

The Enterprise CDSM can operate in two different roles: primary and standby. The primary role is the default. You can have only one primary Enterprise CDSM active in your network; however, you can have any number of Enterprise CDSMs operating in a standby role to provide redundancy and failover capacity. You must configure the primary Enterprise CDSM first. See the [Cisco Enterprise Content Delivery System Quick Start Guide](#) for information on configuring the primary Enterprise CDSM.



Note

The primary and standby Enterprise CDSMs must be running the same version of software. You must upgrade your standby Enterprise CDSM first, and then upgrade your primary Enterprise CDSM.

If the primary Enterprise CDSM is down, the devices (SE and SR) cannot send regular reports and events to it, so the data is sent to the standby Enterprise CDSM. After the primary Enterprise CDSM is online, the database on the standby Enterprise CDSM is synchronized with the database on the primary Enterprise CDSM.

If the primary and secondary Enterprise CDSMs are located in different time zones, the secondary Enterprise CDSM must be configured with the same time zone as the primary Enterprise CDSM. If using NTP to provide time services, the secondary Enterprise CDSM must be configured with the same NTP source and time zone as the primary Enterprise CDSM.

To configure a standby Enterprise CDSM using CLI:

- Step 1** Follow the instructions for configuring a Enterprise CDSM using the setup utility, except do not enter the IP address of the Enterprise CDSM. The instructions can be found in the [Cisco Enterprise Content Delivery System Quick Start Guide](#).
- Step 2** Configure the standby Enterprise CDSM.

```
MDE(config)# cdsd role standby
```
- Step 3** Identify the IP address of the primary CDSM.

```
MDE(config)# cdsd ip 10.1.1.90
```
- Step 4** Start the Centralized Management System (CMS).

```
MDE(config)# cms enable
```
- Step 5** Save the configuration.

```
MDE# copy running-config startup-config
```

- Step 6** Activate the standby Enterprise CDSM by using the web interface of the primary Enterprise CDSM. The primary Enterprise CDSM notifies all registered devices that a standby Enterprise CDSM exists and sends each device the information it needs to contact the standby should the primary fail or become inactive.

**Note**

You cannot log in to the web interface of the standby Enterprise CDSM. Its function is to maintain an up-to-date copy of the primary's database.

Changing a Standby to a Primary Enterprise CDSM

**Note**

If your primary Enterprise CDSM is still operating, you must change its role to standby by executing the **cdsm role standby** command before following these steps. You can only have one primary Enterprise CDSM operating at any given time.

To change the standby Enterprise CDSM to become the primary:

- Step 1** If your primary Enterprise CDSM has failed, enter the following command:
- ```
MDE(config)# cdsm role primary
```
- Step 2** Save the configuration.
- ```
MDE# copy running-config startup-config
```
- Step 3** Restore the old primary Enterprise CDSM, if possible.
- Step 4** When the old primary Enterprise CDSM is restored, change its role to standby.
- ```
cdsm role standby
```
- Step 5** Reconnect the old primary Enterprise CDSM (now standby Enterprise CDSM) into the ECDS network.
- Step 6** Wait at least one polling interval to allow the data from the primary Enterprise CDSM to be copied to the standby Enterprise CDSM.

**Note**

During this period, do not make any configuration changes.

- Step 7** When the new primary Enterprise CDSM and the new standby Enterprise CDSM have synchronized, you can change the roles of the Enterprise CDSMs back to their original roles.

**Note**

There can only be one primary Enterprise CDSM in an ECDS at one time. If there are two primary Enterprise CDSMs, both Enterprise CDSMs are halted.

To do this:

- a. Change the role of the primary Enterprise CDSM to standby.

```
cdsm role standby
```

- b. Change the role of the standby Enterprise CDSM to primary.

```
cdsm role primary
```



**Note** If you have recently made configuration changes to the primary Enterprise CDSM, wait at least the polling interval before changing roles to ensure that the standby has a record of the most recent configuration changes.

- Step 8** If your secondary CDSM is still holding the old node ID, remove the old node ID by entering **cms deregister force**.



**Tip** Similarly, if you are changing from a primary back to a standby CDSM, you may need to use the **cms deregister force** command if the original standby CDSM continues to hold the old node ID.

The following example shows how to use the **cms deregister force** command to release the old node ID:

```
SE# conf t
SE(config)# no cms enable
SE(config)# exit
SE# cms deregister force
SE# wr
SE# conf t
SE(config)# cms enable
```

## Recovering from Two Primary Enterprise CDSMs

If you did not change the primary Enterprise CDSM to standby before you changed the standby Enterprise CDSM to primary, you will have two primary Enterprise CDSMs in your ECDS and both will be halted. To restore both Enterprise CDSMs:

- Step 1** Make sure the Enterprise CDSM that is to be designated as the standby is in fact the standby by entering the **cdsm role standby** command.
- Step 2** Initiate the CMS on the standby Enterprise CDSM by entering the **cms enable** command.
- Step 3** Make sure the Enterprise CDSM that is to be designated as the primary is in fact the primary by entering the **cdsm role primary** command.
- Step 4** Initiate the CMS on the primary Enterprise CDSM by entering the **cms enable** command.
- Step 5** Make sure the standby Enterprise CDSM is activated by using the web interface of the primary Enterprise CDSM.

# Typical Configuration Workflow

Once you have completed activating and configuring the NTP servers for all the devices in the Enterprise CDSM, you are ready to configure the ECDS for content delivery. For information about activating and configuring the NTP servers for a device, see the [“Activating and Setting NTP for Each Device” section on page 3-3](#).

[Table 3-2](#) lists the basic tasks for configuring the ECDS for content delivery, with references to the associated sections in each chapter.

**Table 3-2 Configuration Workflow**

| Task                                               | Description                                                                                                                           | Where to Find More Information                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change admin password                              | Change the administrator password on each device, including the Enterprise CDSM, and change the administrator password for the system | Log in to the CLI for the device and use the <b>username admin password &lt;password&gt;</b> global configuration command.<br><br>The password strength must be a combination of alphabetic characters, at least one number, at least one special character, and at least one uppercase character.<br><br>To change the password for the Enterprise CDSM GUI and CLI, go to <a href="#">“Creating, Editing, and Deleting Users,” page 9-2</a> |
| Configure Dedicated Management with Redundant Port | Separate management traffic from application traffic, and configure a redundant port for management                                   | <a href="#">“Configuring Port Channel and Load Balancing Settings,” page 5-83</a>                                                                                                                                                                                                                                                                                                                                                             |
| Create Device Groups                               | Group like devices to speed up configuration                                                                                          | <a href="#">“Configuring Device Groups,” page 4-3</a>                                                                                                                                                                                                                                                                                                                                                                                         |
| Configure Web Engine                               | For all SEs participating in delivering content                                                                                       | Begins with <a href="#">“Configuring Web Engine HTTP Connections,” page 5-39</a>                                                                                                                                                                                                                                                                                                                                                              |
| Configure Windows Media Engine                     | For all SEs participating in delivering Windows Media content                                                                         | Begins with <a href="#">“Configuring Windows Media Streaming,” page 5-25</a>                                                                                                                                                                                                                                                                                                                                                                  |
| Configure Movie Streamer                           | For all SEs participating in delivering MPEG or MOV content                                                                           | <a href="#">“Configuring Movie Streamer General Settings,” page 5-35</a>                                                                                                                                                                                                                                                                                                                                                                      |
| Configure Flash Media Streaming                    | For all SEs participating in delivering Flash Media Streaming content                                                                 | <a href="#">“Configuring Flash Media Streaming,” page 5-37</a>                                                                                                                                                                                                                                                                                                                                                                                |
| Create Coverage Zone File                          | Map SEs to client service areas by IP address or geographic location                                                                  | <a href="#">Appendix C, “Creating Coverage Zone Files”</a>                                                                                                                                                                                                                                                                                                                                                                                    |
| Import or Upload Coverage Zone File                | Apply Coverage Zone mappings to ECDS                                                                                                  | <a href="#">“Coverage Zone File Registration,” page 9-11</a>                                                                                                                                                                                                                                                                                                                                                                                  |
| Configure Global Routing Method                    | Set the Coverage Zone file                                                                                                            | <a href="#">“Configuring Global Routing,” page 9-13</a>                                                                                                                                                                                                                                                                                                                                                                                       |

**Table 3-2** Configuration Workflow (continued)

| Task                                | Description                                                                      | Where to Find More Information                             |
|-------------------------------------|----------------------------------------------------------------------------------|------------------------------------------------------------|
| Configure Routing Method            | Configure the routing method used by SRs                                         | <a href="#">“Configuring the Service Router,” page 6-1</a> |
| Configure Content Origins           | Define all origin servers that are used in delivery services                     | <a href="#">“Content Origins,” page 8-1</a>                |
| Create Delivery Service Definitions | Create delivery services for both prefetched or cached content and live programs | <a href="#">“Creating Delivery Service,” page 8-4</a>      |
| Create Live Programs                | Create live programs, or rebroadcasts and schedules                              | <a href="#">“Configuring Programs,” page 8-25</a>          |

## Where to Go Next

Proceed to [Chapter 4, “Configuring Devices”](#) to configure locations and device groups for devices, and to configure different types of devices.

**Tip**

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Configuration Guide on Cisco.com.







# CHAPTER 4

## Configuring Devices

The following sections describe how to configure locations and device groups for devices, and provides detailed instructions for configuring the different types of devices:

- [Configuring Locations, page 4-1](#)
- [Configuring Device Groups, page 4-3](#)
- [Configuring the Enterprise CDSM, page 4-9](#)
- [Where to Go Next, page 4-10](#)

## Configuring Locations

Locations are set up in the Enterprise CDSM to organize and group SEs into virtual networks for distribution of content through delivery services. For more information about locations, see the [“Cisco ECDS Topology” section on page 2-2](#).

Locations need to be configured before you can activate SEs and SRs and bring them online in the ECDS network. [Table 4-1](#) describes the icons for the Locations Table page.

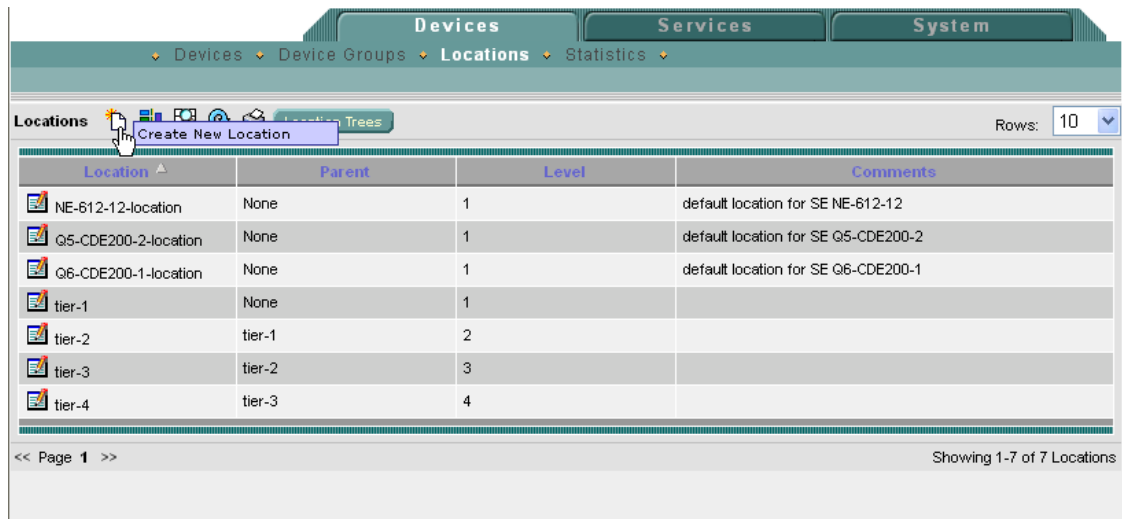
**Table 4-1**      **Location Icons**

| Icon | Function                  |
|------|---------------------------|
|      | Create a new location.    |
|      | Create a filtered table.  |
|      | View all locations.       |
|      | Refresh the table.        |
|      | Print the current window. |
|      | Edit a location.          |

To create a new location or edit an existing one:

- Step 1** Choose **Devices > Locations**. The Locations Table page is displayed (Figure 4-1).  
Sort the table by clicking the column headings.

**Figure 4-1** Locations Table Page



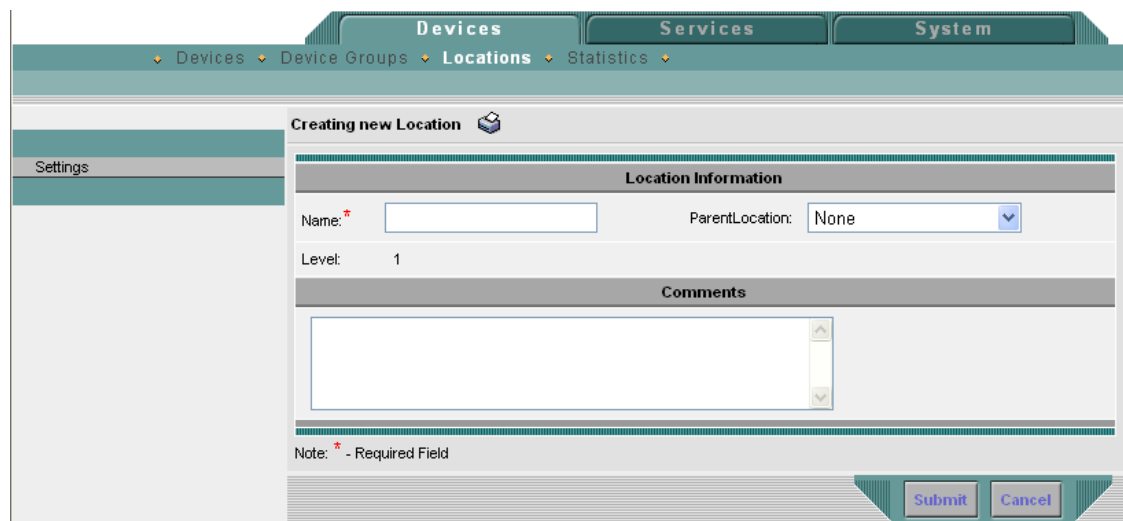
| Location             | Parent | Level | Comments                            |
|----------------------|--------|-------|-------------------------------------|
| NE-612-12-location   | None   | 1     | default location for SE NE-612-12   |
| Q5-CDE200-2-location | None   | 1     | default location for SE Q5-CDE200-2 |
| Q6-CDE200-1-location | None   | 1     | default location for SE Q6-CDE200-1 |
| tier-1               | None   | 1     |                                     |
| tier-2               | tier-1 | 2     |                                     |
| tier-3               | tier-2 | 3     |                                     |
| tier-4               | tier-3 | 4     |                                     |

<< Page 1 >> Showing 1-7 of 7 Locations

- Step 2** In the task bar, click the **Create New Location** icon. The Creating New Location page is displayed (Figure 4-2).

To edit a location, click the **Edit** icon next to the location name.

**Figure 4-2** Creating New Location Page



**Creating new Location**

**Location Information**

Name: \*  ParentLocation:

Level:

**Comments**

Note: \* - Required Field

- Step 3** Enter the settings as appropriate. See Table 4-2 for a description of the fields.

**Table 4-2**      **Location Fields**

| Field           | Description                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name            | Name of the location.                                                                                                                                       |
| Parent Location | Choose a location from the drop-down list. A location with no parent, None, is level 1. The location level is displayed after you choose a parent location. |
| Comments        | Enter any information about the location.                                                                                                                   |

**Step 4** Click **Submit** to save the settings.

To delete a location, from the Locations Table page, click the **Edit** icon next to the location you want to delete, and click the **Delete** icon in the task bar.

To view the location tree, click the **Location Trees** icon in the task bar. The location tree represents the network topology you configured when you assigned a parent to each location.

## Configuring Device Groups

The Enterprise CDSM allows you to configure SEs into device groups so that the entire group of SEs is configured at one time. Device groups and SEs share the same configuration features and options.

[Table 4-3](#) describes the icons for the Device Groups Table page.

**Table 4-3**      **Device Group Table Icons**

| Icon                                                                                | Function                    |
|-------------------------------------------------------------------------------------|-----------------------------|
|  | Creates a new device group. |
|  | Creates a filtered table.   |
|  | Views all device groups.    |
|  | Refreshes the table.        |
|  | Prints the current window.  |
|  | Edits a device group.       |

This section covers creating, editing, and deleting device groups. All other configuration pages for a device group are covered in the [“Configuring the Enterprise CDSM”](#) section on page 4-9.

To create or edit a device group:

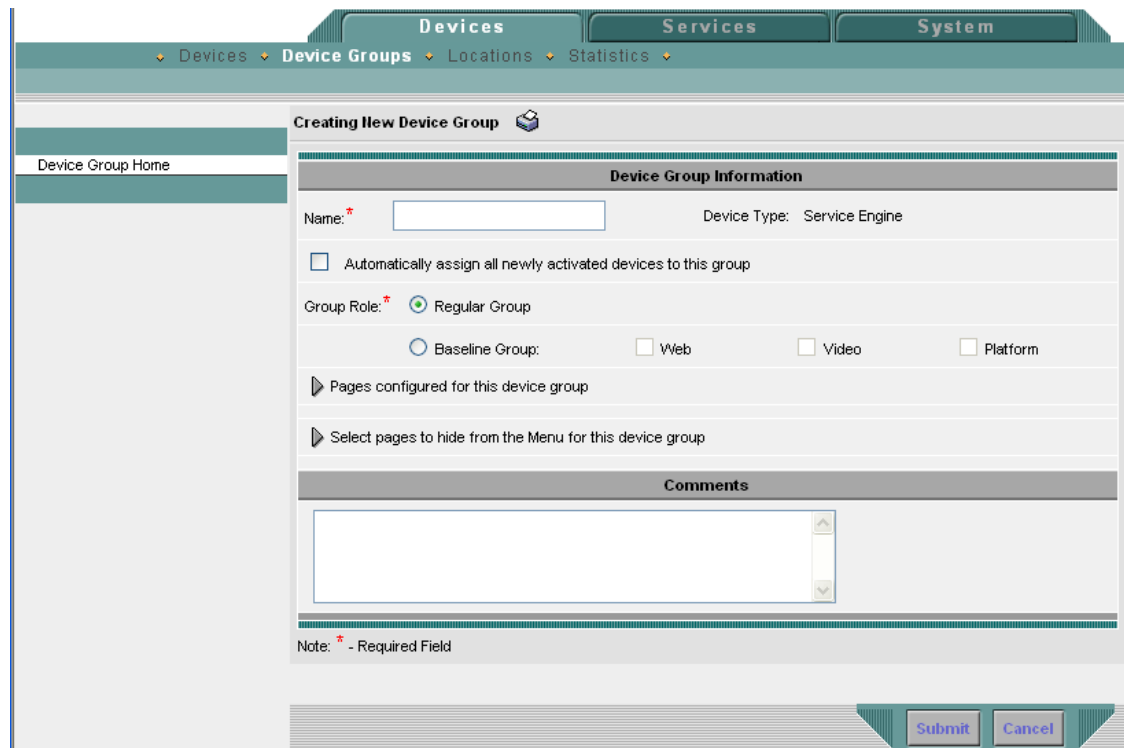
- Step 1** Choose **Devices > Device Groups**. The Device Groups Table page is displayed (Figure 4-3).  
Sort the table by clicking the column headings.

**Figure 4-3** Device Groups Table Page



- Step 2** In the task bar, click the **Create New Device Group** icon. The Creating New Device Group page is displayed (Figure 4-4).  
To edit a device group, click the **Edit** icon next to the device group name.

**Figure 4-4** Creating New Device Group Page



- Step 3** In the Name field, enter the name of the device group. The name must be unique and should be a name that is useful in distinguishing the device group from the others in the ECDS.
- Step 4** Check the **Automatically assign all newly activated devices to this group** check box if applicable.

- Step 5** Choose **Regular Group** to indicate this group is not used as a baseline for all SEs or choose **Baseline Group** and select the baseline type to define this group as a baseline for all SEs.
- For information about baseline groups, see the [“Baseline Groups” section on page 2-3](#).
- Step 6** To customize the left panel menu for this device group, click the **Select pages to hide from the menu for this device group** arrow, and check the pages you want to hide. To collapse these settings, click the arrow again.
- Use this feature to remove from view any configuration pages that you do not need for the device group.
- Step 7** In the Comments field, enter any information about the device group.
- Step 8** Click **Submit** to save the settings.
- If you are editing this device group, you can view a list of all settings configured for this device group by clicking the **Pages configured for this device group** arrow. To collapse this information list, click the arrow again.
- To delete a device group, click the **Delete** icon in the task bar.
- Step 9** To assign SEs to the device group, choose **Assignments > Devices**. The Assignment table is displayed listing all SEs in the ECDS.

**Note**

From this point forward, the steps to get to a configuration page are combined into one step using notation similar to the following: **Device Group > Assignments > Devices**.

- Step 10** Click the **Assign** icon (blue cross mark) next to each SE name you want to assign to this group.
- To assign all SEs, click **Assign all Service Engines** in the task bar.
- Step 11** Click **Submit** to add the selected SEs to the device group.

**Tip**

Verify individual devices in your newly created device group to ensure that they have been configured correctly. See [Verifying Devices in Device Groups](#).

- To remove an SE from the device group, click the **Unassign** icon (green check mark) next to the name of the SE, and click **Submit**.
- To remove all SEs from the device group, click the **Unassign all Service Engines** icon in the task bar, and click **Submit**.

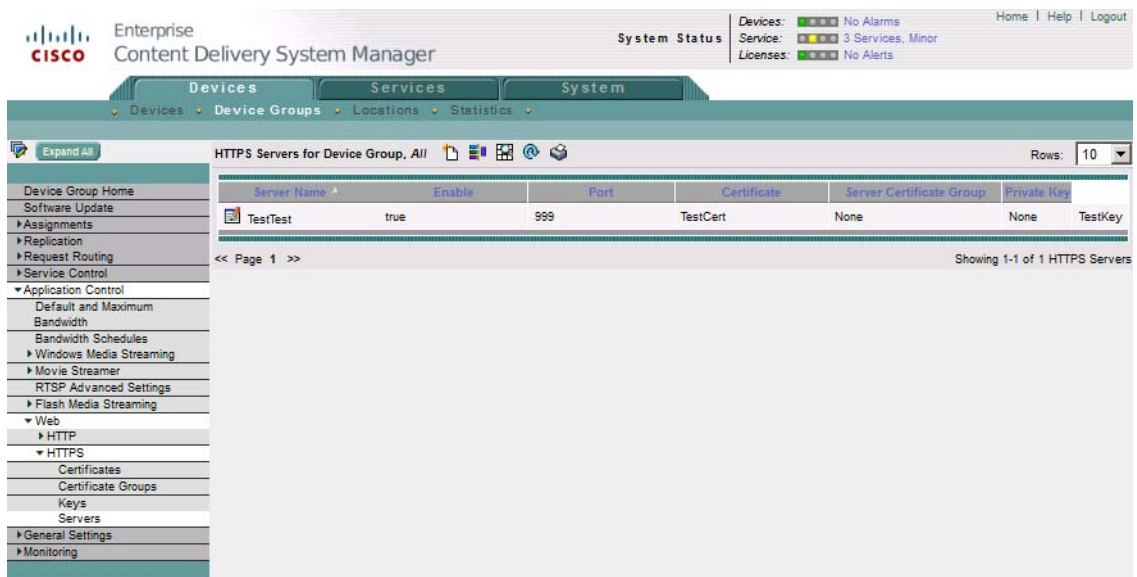
## Working with Device Groups

- [Verifying Devices in Device Groups, page 4-6](#)
- [Managing New Device Groups, page 4-6](#)
- [Managing Aggregate Settings, page 4-8](#)
- [Managing Device Group Overlap, page 4-9](#)

## Verifying Devices in Device Groups

Once the configuration is successfully set for a device group, the system displays the intended configuration of the entire device group rather than the status of individual devices within the group. For example, [Figure 4-5](#) shows that the TestTest device group is successfully created in the Enable (True) column. However, it is recommended that you verify that all devices within your device group are successfully configured by running the **show config** commands for each device on the Service Engine. If any error is found on the device using the CLI, reconfigure that device by returning to the ECDS administration GUI. Any subsequent changes that you make to your Service Engine configuration should be verified using the CLI and corrected using the ECDS administration GUI.

**Figure 4-5** Successfully Configured Device Group



## Managing New Device Groups

When you first create a device group, all settings you configure for the device group are automatically propagated to all the SEs assigned to that group.



### Note

All SE settings in the “[Configuring the Enterprise CDSM](#)” section on [page 4-9](#), except those listed below, can also be configured for a device group. The following pages are not available for device group configuration:

- **Devices > Application Control > Windows Media Streaming > Bypass List.** See the “[Configuring the Windows Media Outgoing Proxy Bypass List](#)” section on [page 5-32](#) for more information.
- **Devices > General Settings > Network > Network Interfaces.** See the “[Viewing Network Interfaces](#)” section on [page 5-82](#) for more information.
- **Devices > General Settings > Network > External IP.** See the “[Configuring External IP Addresses](#)” section on [page 5-82](#) for more information.
- **Devices > General Settings > Network > IP ACL.** See the “[Configuring IP ACL](#)” section on [page 5-84](#) for more information.

After configuring the device group settings, the task bar for the corresponding configuration page for an individual SE that is part of that device group displays the **Override Group Settings** icon and the Device Group drop-down list with the device group name displayed.

When an SE is associated with one or many device groups, the name of the device group whose settings were applied last are displayed.

To configure individual settings for an SE in a device group, click the **Override Group Settings** icon in the task bar. You can then edit the fields on the page and click **Submit**. The Device Group drop-down list displays “Select a Device Group.”

To reapply the settings for the device group, select the device group from the Device Group drop-down list and click **Submit**. Alternatively, you can go to the corresponding device group configuration page and click the **Force Settings on SEs in Group**. The **Force Settings on SEs in Group** only displays for a device group configuration page when an SE’s individual settings override the group settings.

**Note**

The individual SE configuration page does not display the **Override Group Settings** icon and Device Group drop-down list in the task bar if the settings have not been configured for the corresponding device group configuration page.

To force all device group settings to all assigned SEs, go to the Device Group Home page and click the **Force Group Settings** icon in the task bar.

**Note**

The last configuration submitted for the device, whether it is the device group configuration or the individual device configuration, is the configuration the device uses.

Table 4-4 describes the icons for the Device Groups configuration pages.

**Table 4-4**      **Device Group Configuration Icons**

| Icon                                                                                | Function                                                                                                                                |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|  | Deletes a device group.                                                                                                                 |
|  | Updates application statistics.                                                                                                         |
|  | Forces full database update.                                                                                                            |
|  | Reboots all devices in device group.                                                                                                    |
|  | Forces the group settings. Forces the complete set of configurations made for a device group to all devices associated with that group. |
|  | Forces settings on SEs in a device group. Forces the configuration of the displayed page to all SEs in the device group.                |
|  | Overrides the group settings on the device.                                                                                             |
|  | Prints the current window.                                                                                                              |

## Managing Aggregate Settings

The following device and device group configuration pages have aggregate settings:

- **Replication > Scheduled Bandwidth.** See the “[Scheduled Bandwidth](#)” section on page 5-8 for more information.
- **Service Control > Service Rules.** See the “[Configuring Service Rules](#)” section on page 5-11 for more information.
- **Application Control > Bandwidth Schedules.** See the “[Configuring Bandwidth Schedules](#)” section on page 5-23 for more information.
- **General Settings > Login Access Control > Users > Usernames.** See the “[Creating, Editing, and Deleting Users—Usernames](#)” section on page 5-70 for more information.

To access these pages, first choose **Devices > Devices** or **Devices > Device Groups**, followed by the **Edit** icon next to the device or device group you want to configure.

Aggregate Settings is set to **Yes** by default. When Aggregate Settings is set to **Yes**, the settings for the device group are aggregated with the settings for the SE. This means you can configure settings for all SEs in a device group, then configure individual settings for each SE, and the combined settings for the device group and individual SE are apply to the SE. Any settings for the device group are listed with the **View** icon and any settings for the individual SE are listed with the **Edit** icon on the individual SE configuration page.

If Aggregate Settings is set to **No**, only the individual SE settings are applied to the SE and the device group settings do not apply to the SE.

To edit the device group settings, or configure new settings for the device group, you must go to the device group corresponding configuration page.

If you remove all device group settings, all device settings displayed with Aggregate Settings enabled are removed as well.



**Note** The last configuration submitted for the device, whether it is the device group configuration or the individual device configuration, is the configuration the device uses.

[Table 4-4](#) describes the icons for the configuration pages that have aggregate settings.

**Table 4-5 Aggregate Settings Icons**

| Icon | Function                                                              |
|------|-----------------------------------------------------------------------|
|      | Creates a new entry.                                                  |
|      | Edits an entry.                                                       |
|      | Deletes an entry.                                                     |
|      | Views read-only entry.                                                |
|      | Creates a filtered table. Filter the table based on the field values. |



**Table 4-5 Aggregate Settings Icons (continued)**

| Icon                                                                              | Function                                                                                              |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
|  | Views all table entries. Click this icon to view all entries after you have created a filtered table. |
|  | Refreshes the table.                                                                                  |
|  | Prints the current window.                                                                            |

## Managing Device Group Overlap

If you want the ability to assign a device to more than one device group, you must enable device group overlap. Device group overlap is enabled by default.

To enable or disable device group overlap:

- 
- Step 1** Choose **System > Configuration**. The Config Properties page is displayed.
- Step 2** Click the **Edit** icon next to the DeviceGroup.overlap property. The Modifying Config Property page is displayed.
- Step 3** To enable device group overlap, choose **true** from the **Value** drop-down list.  
To disable device group overlap, choose **false** from the **Value** drop-down list.
- Step 4** Click **Submit** to save the settings.

You cannot disable device group overlap after you have assigned devices to multiple device groups.



**Tip** To force the complete configuration set of a device group to all devices in that group, click the **Force Group Settings** icon in the task bar.

---

## Configuring the Enterprise CDSM

Configure the Cisco Enterprise CDSM using the General Settings menu. See the [“General Settings” section on page 5-64](#).

Device activation is accomplished during installation and initialization of the Cisco Media Delivery Engine (MDE) devices. For more information about initially configuring the Cisco MDEs, see the [Cisco Enterprise Content Delivery System Quick Start Guide](#).

The Device Activation page for the CDSM displays information about the management IP address and the role of the CDSM. To change the name of the CDSM:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.

**Step 4** Choose **Device Activation**. The General Information page displays.

**Step 5** Enter a new name in the **Name** field and click **Submit**.

**Tip**

For information about primary and standby CDSMs, see the [“Configuring Primary and Standby Enterprise CDSMs” section on page 3-11](#).

---

## Where to Go Next

Proceed to [Chapter 5, “Configuring the Service Engine”](#) to activate your Service Engine, assign devices to device groups, manage service and application control, and maintain general settings for the SE.

**Tip**

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Configuration Guide on Cisco.com.

---



## CHAPTER 5

# Configuring the Service Engine

---

The following sections describe how to configure a Service Engine:

- [Activating a Service Engine, page 5-1](#)
- [Assigning Devices to Device Groups, page 5-5](#)
- [Configuring Bandwidth for Replication and Ingest, page 5-6](#)
- [Service Control, page 5-11](#)
- [Application Control, page 5-22](#)
- [General Settings, page 5-64](#)
- [Where to Go Next, page 5-110](#)

## Activating a Service Engine

Activating a device (Service Engine, Service Router, or CDSM) can be done through the Devices home page initially, or through the Device Activation page.

To activate a device from the Device Activation page:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed ([Figure 5-1](#)).

Figure 5-1 Devices Table Page

| Devices                                                                     |                                           |            |         |                      |                  |
|-----------------------------------------------------------------------------|-------------------------------------------|------------|---------|----------------------|------------------|
| Devices ▾ Device Groups ▾ Locations ▾ Statistics ▾                          |                                           |            |         |                      |                  |
| <div> <div>Devices</div> <div> </div> </div> <div>Rows: 10 ▾</div>          |                                           |            |         |                      |                  |
| Device Name ▲                                                               | Type                                      | IP Address | Status  | Location             | Software Version |
| NE-612-12                                                                   | Service Engine                            | 3.1.4.31   | Online  | NE-612-12-location   | 2.0.0.b.450      |
| NE-612-5                                                                    | Service Engine                            | 3.1.4.14   | Online  | tier-1               | 2.0.0.b.470      |
| NE-612-6                                                                    | Service Engine                            | 3.1.4.15   | Online  | NE-612-12-location   | 2.0.0.b.470      |
| NE-612-7                                                                    | Service Engine                            | 3.1.4.16   | Online  | tier-1               | 2.0.0.b.470      |
| NE-7326-2                                                                   | Service Engine                            | 3.1.4.21   | Online  | tier-3               | 2.0.0.b.470      |
| NE-CDM-612-9                                                                | Content Delivery System Manager (Primary) | 3.1.4.18   | Online  |                      | 2.0.0.b.470      |
| NE-CR-612-4                                                                 | Service Router                            | 3.1.4.13   | Online  | tier-1               | 2.0.0.b.470      |
| Q5-CDE200-1                                                                 | Service Engine                            | 2.225.2.11 | Offline | tier-1               | 2.0.0.b.410      |
| Q5-CDE200-2                                                                 | Service Engine                            | 2.225.2.56 | Offline | Q5-CDE200-2-location | 2.0.0.b.420      |
| Q5-CDE200-4                                                                 | Service Engine                            | 2.225.2.14 | Online  | tier-1               | 2.0.0.b.440      |
| <div>&lt;&lt; Page 1 2 &gt;&gt;</div> <div>Showing 1-10 of 12 Devices</div> |                                           |            |         |                      |                  |

**Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.

**Step 3** Click **Show All** to display the top-level menu options, and click **Device Activation**. The Device Activation page is displayed (Figure 5-2).

Figure 5-2 Device Activation Page

| Devices                                                                                                                                                                                                                                |  | Services            | System |  |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---------------------|--------|--|--|
| Devices ▾ Device Groups ▾ Locations ▾ Statistics ▾                                                                                                                                                                                     |  |                     |        |  |  |
| <div> <div>Expand All</div> <div>Show Basic</div> </div> <div>Device Activation, perf-CDE200-1</div>                                                                                                                                   |  |                     |        |  |  |
| <div> <div>Device Home</div> <div>Device Activation</div> <div>▸ Assignments</div> <div>▸ Replication</div> <div>▸ Service Control</div> <div>▸ Application Control</div> <div>▸ General Settings</div> <div>▸ Monitoring</div> </div> |  |                     |        |  |  |
| <div>General Configuration</div>                                                                                                                                                                                                       |  | <div>Locality</div> |        |  |  |
| Name: perf-CDE200-1                                                                                                                                                                                                                    |  | Location: Loc1 ▾    |        |  |  |
| Status: Online                                                                                                                                                                                                                         |  |                     |        |  |  |
| Activate: <input checked="" type="checkbox"/>                                                                                                                                                                                          |  |                     |        |  |  |
| Server Offload: <input type="checkbox"/>                                                                                                                                                                                               |  |                     |        |  |  |
| Content Cache: 4769210 MB                                                                                                                                                                                                              |  |                     |        |  |  |
| Set Default Coverage Zone File: <input type="checkbox"/>                                                                                                                                                                               |  |                     |        |  |  |
| Management Communication Configuration                                                                                                                                                                                                 |  |                     |        |  |  |
| <input checked="" type="checkbox"/> Use SE's primary IP Address for Management Communication                                                                                                                                           |  |                     |        |  |  |
| Management Communication Address: <input type="text"/>                                                                                                                                                                                 |  |                     |        |  |  |
| Management Communication Port: 443                                                                                                                                                                                                     |  |                     |        |  |  |
| Comments                                                                                                                                                                                                                               |  |                     |        |  |  |
| n/a                                                                                                                                                                                                                                    |  |                     |        |  |  |
| Note: * - Required Field                                                                                                                                                                                                               |  |                     |        |  |  |
| <div>Submit Cancel</div>                                                                                                                                                                                                               |  |                     |        |  |  |

**Step 4** Enter the settings as appropriate. See [Table 5-1](#) for a description of the fields.

**Table 5-1** *Device Activation Fields*

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name           | Name of the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Activate       | <p>To activate or deactivate the device, check or uncheck the <b>Activate</b> check box. Alternatively, you can click the <b>Deactivate Device</b> icon in the task bar.</p> <p>When you uncheck the <b>Activate</b> check box and click <b>Submit</b>, the <b>Replaceable</b> check box is displayed. Check the <b>Replaceable</b> check box when you need to replace the device or recover lost registration information. For more information, see the “<a href="#">Recovering ECDS Network Device Registration Information</a>” section on <a href="#">page 11-18</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server Offload | <p>To offload this device for maintenance or a software upgrade, check the <b>Server Offload</b> check box. When checked, the Service Router stops sending requests to this device.</p> <p><b>Note</b> If a client paused a program at that moment <b>Server Offload</b> is enabled, most likely resuming the program will fail.</p> <p>To monitor the current streams on an SE during the Server Offload state, use the <b>show interface</b> command. If the packets received or packets sent is increasing then the SE is streaming. The number of packets received is high if there is an incoming stream.</p> <p><b>Note</b> We recommend separating the management traffic from the streaming traffic by using the port channel configuration.</p> <ul style="list-style-type: none"> <li>• If management and streaming traffic are separated, the <b>show interface</b> command for the streaming port channel displays information on active sessions.</li> <li>• If management and streaming traffic are not separated, the <b>show interface</b> command shows very low traffic; the packets received and packets sent are lower than a client streaming session.</li> </ul> <p>Once the SE has finished streaming, you can perform maintenance or upgrade the software on the device. For information about upgrading the software, see the “<a href="#">Upgrading Software</a>” section on <a href="#">page 11-1</a>.</p> <p>The Status field on the Device Activation page and the Devices Table page displays “offloading” when <b>Server Offload</b> is checked.</p> <p>Once the software upgrade or maintenance is complete, you need to uncheck the <b>Server Offload</b> check box so that the device can again participate in the system.</p> <p><b>Note</b> If the Server Offload option is set on an SE that is acting as the Content Acquirer for a delivery service for dynamic ingest or live stream splitting, a new SE is chosen as the Location Leader for the delivery service. However, if the Content Acquirer is up and communicating with the CDSM, it continues to perform content ingest and content distribution.</p> |

**Table 5-1**      **Device Activation Fields (continued)**

| Field                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Content Cache                    | Informational only. The content cache size is the total disk space on the ECDS network file system (CDNFS) on the SE that is designated for cache. The Content Cache represents the unused cache space. The used cache space is the disk space allotted for all the delivery services to which the SE is assigned. To view the used cache space, choose <b>Services &gt; Service Definition &gt; Delivery Services &gt; Assign Service Engines</b> .                                                                                                                                                                                                                                      |
| Set Default Coverage Zone File   | <p>When checked, which is the default setting, a default Coverage Zone file is generated with the SE serving the local subnet it resides on. The coverage zone is an ECDS network-wide mapping of client IP addresses to SE IP addresses that should respond to client requests. For more information, see the <a href="#">“Coverage Zone File Registration”</a> section on page 9-11.</p> <p>The default coverage zone can be disabled and you can create and assign custom coverage zones using the Coverage Zone file import or upload.</p> <p>Uncheck the <b>Set Default Coverage Zone File</b> check box to use a user-defined Coverage Zone file that was imported or uploaded.</p> |
| Location                         | Lists all the locations configured for the ECDS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Use SE’s primary IP address      | <p>Enables the CDSM to use the IP address on the primary interface of the SE for management communications.</p> <p><b>Note</b> If the <b>Use SE’s primary IP Address for Management Communication</b> check box is checked and the Management Communication Address and Port are configured, the CDSM uses the SE’s primary IP address for communication.</p> <p><b>Note</b> Do not check the <b>Use SE’s primary IP Address for Management Communication</b> check box if you want to separate management and streaming traffic. Instead, use the Management Communication Address and Port fields to specify where management traffic should be sent.</p>                               |
| Management Communication Address | <p>Manually configures a management IP address for the CDSM to communicate with the SE.</p> <p>Manual configuration of the management IP address and port are used when using port channel configuration to separate management and streaming traffic. For more information about port channel configuration see the <a href="#">“Configuring Port Channel and Load Balancing Settings”</a> section on page 5-83.</p>                                                                                                                                                                                                                                                                     |
| Management Communication Port    | Port number to enable communication between the CDSM and the SE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Comments                         | Information about the settings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**Step 5** Click **Submit** to save the settings.

# Assigning Devices to Device Groups

You can assign devices to device groups in three ways:

- Through the Device Group Assignment page
- Through the device Assignment page
- Through the Devices home page, if the device group is a baseline group

To assign devices to device groups through the Assignment page:

- Step 1** Choose **Devices > Devices**, and click the **Edit** icon next to the device you want to assign.
- Step 2** Click **Show All**, and then choose **Assignments > Device Groups**. The Device Group Table page is displayed with all of the configured device groups listed (Figure 5-3).



**Note** From this point forward, the beginning steps in the procedures are combined into one step using notation similar to the following: **Devices > Devices Assignments > Device Groups**.

**Figure 5-3 Assignment Page**



- Step 3** Click the **Assign** icon (blue cross mark) next to the device group you want to assign to this SE. Alternatively, click the **Assign All Device Groups** icon in the task bar.

A green arrow wrapped around the blue X indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon. The SE assignment states are described in Figure 5-4.

**Figure 5-4 SE Assignment State**

|            |                                 |                      |                               |                                                                                            |
|------------|---------------------------------|----------------------|-------------------------------|--------------------------------------------------------------------------------------------|
| New Assign | Assigned and waiting for Submit | Assignment Submitted | Unassign Submitted Assignment | Not modifiable. The quota on all the delivery services for this SE exceeds the disk space. |
|            |                                 |                      |                               |                                                                                            |

- Step 4** Click **Submit** to save the settings.

A green circle with a check mark indicates a device group is assigned to this SE. To unassign the device group, click this icon, or click the **Remove All Device Groups** icon in the task bar. Click **Submit** to save the changes.

Additionally, the **Filter Table** icon and **View All Device Groups** icon allow you to first filter a table and then view all device groups again.

## Configuring Bandwidth for Replication and Ingest

The bandwidth used for replication and ingest is determined by the configuring the settings on the following pages:

- [Default Bandwidth, page 5-7](#)
- [Scheduled Bandwidth, page 5-8](#)



**Tip**

View a graphical representation of the bandwidth settings using the **Display Graph** icon in the tool bar. See the [“Bandwidth Graph” section on page 5-10](#) for more information.

[Table 5-2](#) describes the icons on the replication bandwidth configuration pages.

**Table 5-2 Replication Bandwidth Configuration Icons**

| Icon                                                                                | Function                                                                                                                |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
|  | Refreshes the table or page.                                                                                            |
|  | Displays a graph.                                                                                                       |
|  | Applies the default settings to the device.                                                                             |
|  | Creates a new item.                                                                                                     |
|  | Creates a filtered table. Filter the scheduled bandwidth by start time, end time, days of the week, and bandwidth type. |
|  | Views all scheduled bandwidth. Click this icon to view all schedule bandwidths after you have created a filtered table. |
|  | Prints the current window.                                                                                              |
|  | Edits a scheduled bandwidth. Click this icon next to one of the scheduled bandwidths to edit the settings.              |
|  | Deletes a scheduled bandwidth. To delete a scheduled bandwidth, click the <b>Edit</b> icon and then click this icon.    |

**Tip** For more information about task bar icons, see the [“Task Bar” section on page 3-9](#).



## Default Bandwidth

The default bandwidth settings can be configured for acquisition (ingest) and distribution (replication) of content. The default settings are used unless a scheduled bandwidth is configured for a specified time period.

To set the default bandwidth for replication:

- Step 1** Choose **Devices > Devices > Replication > Default Bandwidth**. The Replication Default Bandwidth page is displayed (Figure 5-5).

**Figure 5-5** Replication Default Bandwidth Page

- Step 2** Enter the settings as appropriate. See Table 5-3 for a description of the fields.

**Table 5-3** Replication Default Bandwidth Fields

| Field                      | Description                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Acquisition-in Bandwidth   | Bandwidth used for ingesting content when this SE is acting as the Content Acquirer.<br>The default is 500 Mbps (megabits per second). |
| Distribution-in Bandwidth  | Bandwidth used for incoming content that is sent by a forwarding SE as part of the distribution process.<br>The default is 250 Mbps.   |
| Distribution-out Bandwidth | Bandwidth used for outgoing content that is sent to a downstream SE as part of the distribution process.<br>The default is 500 Mbps.   |

- Step 3** Click **Submit** to save the settings.

## Scheduled Bandwidth

Scheduled Bandwidth settings take precedence over Default Bandwidth settings. To configure a bandwidth schedule:

- Step 1** Choose **Devices > Devices > Replication > Scheduled Bandwidth**. The Replication Scheduled Bandwidth Table page is displayed (Figure 5-6).

The table is sortable by clicking the column headings.

**Figure 5-6** Replication Scheduled Bandwidth Table Page

| Start Time | End Time | Day(s) of Week | Bandwidth Type  | Bandwidth Rate (Kbps) |
|------------|----------|----------------|-----------------|-----------------------|
| 02:00      | 05:00    | SuMoTuWeThFrSa | AcquisitionIn   | 500000                |
| 02:00      | 05:00    | SuMoTuWeThFrSa | DistributionIn  | 500000                |
| 02:00      | 05:00    | SuMoTuWeThFrSa | DistributionOut | 500000                |

For information about Aggregate Settings, see the “[Managing Aggregate Settings](#)” section on page 4-8.



**Note** Configuring Replication Bandwidth Scheduling is only supported on a per SE-basis; Device Group configuration of Replication Bandwidth Scheduling is not supported.

- Step 2** Click the **Create New** icon in the task bar. The Replication Scheduled Bandwidth page is displayed (Figure 5-7).
- Step 3** To edit a scheduled bandwidth, click the **Edit** icon next to the scheduled bandwidth you want to edit.

**Figure 5-7** Replication Scheduled Bandwidth Page

**Step 4** Enter the settings as appropriate. See [Table 5-4](#) for a description of the fields.

**Table 5-4** Replication Scheduled Bandwidth Fields

| Field          | Description                                                                                                                                                                                                                                                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bandwidth Type | Distribution-in—For incoming content distribution traffic from SEs.<br>Distribution-out—For outgoing content distribution traffic to SEs.<br>Acquisition-in—For incoming content acquisition traffic from origin servers.                                                                                                       |
| Bandwidth Rate | Maximum amount of bandwidth that you want to allow (in kbps).                                                                                                                                                                                                                                                                   |
| Start Time     | Time of day for the bandwidth setting to begin, using a 24-hour clock in local time (hh:mm).                                                                                                                                                                                                                                    |
| End Time       | Time of day for the bandwidth setting to end (hh:mm).                                                                                                                                                                                                                                                                           |
| Day Selection  | Days on which bandwidth settings apply. <ul style="list-style-type: none"> <li>Full Week—Specifies that the allowable bandwidth settings are applied for an entire week.</li> <li>Sun, Mon, Tue, Wed, Thu, Fri, and Sat—Specifies individual days of the week on which the allowable bandwidth settings take effect.</li> </ul> |

**Step 5** Click **Submit** to save the settings.

## Bandwidth Graph

To view a graphical representation of the bandwidth settings, click the **Display Graph** icon in the task bar. The Acquisition and Distribution Bandwidth graph is displayed in a new window.

The vertical axis of the graph represents the amount of bandwidth in Kbps (kilobits per second) and the horizontal axis represents the days of the week. The scale shown on the vertical axis is determined dynamically based on the bandwidth rate for a particular type of bandwidth and is incremented appropriately. The scale shown on the horizontal axis for each day is incremented for each hour. Each type of bandwidth is represented by a unique color. A legend at the bottom of the graph maps the colors to the corresponding bandwidths.

You can change the graph view by choosing the different options, as described in [Table 5-5](#).

**Table 5-5 Acquisition and Distribution Bandwidth Graph—Viewing Options**

| Option                                           | Description                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Distribution In                                  | Bandwidth settings for incoming content distribution traffic. The default is 1,000,000.                                                                                                                                                                                                                                                                                                                   |
| Distribution Out                                 | Bandwidth settings for outgoing content distribution traffic. The default is 500,000.                                                                                                                                                                                                                                                                                                                     |
| Acquisition In                                   | Bandwidth settings for incoming content acquisition traffic. The default is 1,000,000.                                                                                                                                                                                                                                                                                                                    |
| All Servers                                      | A consolidated view of all configured bandwidth types. This is the default.                                                                                                                                                                                                                                                                                                                               |
| Show Detailed Bandwidth/Show Effective Bandwidth | <p>Toggles between the two options:</p> <p>Show Detailed Bandwidth—Displays detailed bandwidth settings for the SE and its associated device groups. The bandwidth settings of the device and device groups are shown in different colors for easy identification.</p> <p>Show Effective Bandwidth—Displays the composite (aggregate) bandwidth settings for the SE and its associated device groups.</p> |
| Show Aggregate View/Show Non-Aggregate View      | <p>Toggles between the two options:</p> <p>Show Aggregate View—Displays the bandwidth settings configured for the corresponding device groups.</p> <p>Show Non-Aggregate View—Displays the bandwidth settings configured for the SE.</p>                                                                                                                                                                  |
| Sun, Mon, Tues, Wed, Thurs, Fri, Sat             | Displays the bandwidth settings for the corresponding day of the week.                                                                                                                                                                                                                                                                                                                                    |
| Full Week                                        | Displays the bandwidth settings for the entire week. This is the default view and is combined with the All Servers view.                                                                                                                                                                                                                                                                                  |

# Service Control

The Service Control pages provide settings for client request filtering and third-party QoS and conditional access policies. Additionally, transaction logs that monitor traffic are configured under the Service Control. Configuring service control consists of the following procedures:

- [Configuring Service Rules, page 5-11](#)
- [Configuring ICAP Services, page 5-18](#)
- [Configuring PCMM QoS Policy, page 5-18](#)
- [Configuring URL Signing, page 5-18](#)
- [Configuring the Authorization Service, page 5-18](#)
- [Configuring Transaction Logging, page 5-19](#)

Table 5-2 describes the icons for the Service Control pages.

**Table 5-6 Service Control Icons**

| Icon                                                                                | Function                                                                                  |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
|    | Refreshes the table or page.                                                              |
|    | Applies the default settings to the device.                                               |
|  | Creates a new item.                                                                       |
|  | Creates a filtered table.                                                                 |
|  | Views all data. Click this icon to view all data after you have created a filtered table. |
|  | Prints the current window.                                                                |
|  | Edits an item.                                                                            |
|  | Deletes an item. To delete an item, click the <b>Edit</b> icon and then click this icon.  |

## Configuring Service Rules

The Rules Template licensed feature provides a flexible mechanism to specify configurable caching requests by allowing these requests to be *matched* against an arbitrary number of parameters, with an arbitrary number of *policies* applied against the matches. You can specify a set of rules, each clearly identified by an action and a pattern. Subsequently, for every incoming request, if a pattern for a rule matches the given request, the corresponding action for that rule is taken.

**Note**

The processing time on the SE is directly related to the number of service rules configured. Processing times increase with an increase in the total number of rules configured. If the SE processing time is greater than twice the datafeed poll rate, then the device goes offline until the processing is completed. You can avoid this by configuring a higher datafeed poll rate. The recommended datafeed poll rate for 750 service rules is 300 seconds. To configure the datafeed poll rate, see the [“Configuring System Settings” section on page 9-7](#).

Configuring a service rule consists of the following tasks:

- Enabling the service rules. (Only needs to be performed once.)
- Configuring a pattern list and adding a pattern to it.
- Associating an action with an existing pattern list.

There are three cases for service rules:

1. If allow rules are configured, then it is an implicit deny.
2. If deny rules are configured, then it is an implicit allow.
3. If both allow and deny rules are configured, then it is an implicit allow.

For example, if all URL requests that match HTML are blocked implicitly, all requests that match other URL requests are allowed.

If all URL requests that match WMV are allowed implicitly, all request that match other URL requests are blocked.

If both of the above rules are configured, then HTML URL requests are blocked, and all other URL requests are allowed.

See the following sections to manage service rules

- [Enabling Service Rules, page 5-12](#)
- [Enabling Apple HTTP Live Streaming, page 5-15](#)
- [Executing Rule Actions in Order, page 5-17](#)

## Enabling Service Rules

### Procedure

To configure or edit service rule settings:

- 
- Step 1** Choose **Devices > Devices > Service Control > Enable Rules**. The Enable Service Rules page is displayed.
- Step 2** Check the **Enable** check box to enable the use of rule settings.
- When you enable service rules, a dialog box displays the following message:
- “Please ensure you have purchased License for this advanced feature”
- Click **OK** and continue to configure your service rules. You do not need to install an additional license to use this feature.
- Step 3** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

- Step 4** Choose **Devices > Devices > Service Control > Service Rules**. The Service Rules Table page is displayed.
- The table is sortable by clicking the column headings. For information about Aggregate Settings, see the [“Managing Aggregate Settings”](#) section on page 4-8.
- Step 5** Click the **Create New** icon in the task bar. The Service Rules page is displayed (Figure 5-8).
- Step 6** To edit a service rule, click the **Edit** icon next to the service rule you want to edit.

**Figure 5-8 Service Rules Page**

- Step 7** Create a pattern list and add a pattern to it.
- From the **Rule Type** drop-down list, choose **pattern-list**.
  - In the **Rule Parameters** field, configure the pattern list number and the pattern type, following the rules usage guidelines shown on the Service Rules page. See [Table 5-7](#) for a description of pattern types. The rule patterns are not case-sensitive.

For example, to create pattern list number 72 with the pattern type *domain* and the yahoo.com domain as the domain to be acted on, enter **72 domain yahoo.com** in the **Rule Parameters** field.

**Table 5-7 Service Rules Pattern Types**

| Pattern Type | Description                                                                                                                                                                                                                                                                                                                                                                                                   | Syntax                                                                    |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| domain       | Matches the domain name in the URL or the host header against a regular expression. For example, “.*ibm.*” matches any domain name that contains the “ibm” substring. “\foo\com\$” matches any domain name that ends with the “.foo.com” substring.<br><br>In regular expression syntax, the dollar sign (\$) metacharacter directs that a match is made only when the pattern is found at the end of a line. | <b>rule pattern-list</b> <i>list_num</i><br><b>domain</b> <i>dn_regex</i> |
| group-type   | Patterns can be combined by using the AND or OR function with the group-type pattern (for example, <b>rule pattern-list 1group-type and</b> ). The default is OR.                                                                                                                                                                                                                                             | <b>rule pattern-list</b> <i>list-num</i><br><b>group-type {and   or}</b>  |

**Table 5-7** Service Rules Pattern Types (continued)

| Pattern Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Syntax                                                                                                                                                                                  |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| header-field | <p>Request header field pattern.</p> <p>Request header field patterns <b>referer</b>, <b>request-line</b>, and <b>user-agent</b> are supported for the allow, block, and redirect actions. The <b>referer</b> pattern is matched against the Referer header in the request, the <b>request-line</b> pattern is matched against the first line of the request, and the <b>user-agent</b> pattern is matched against the User-Agent header in the request. The user-agent pattern is not case sensitive.</p> <p><b>Note</b> Flash Media Streaming supports the <b>referer</b> header field pattern for the allow and block actions.</p> | <b>rule pattern-list</b> <i>list_num</i><br><b>header-field</b> { <b>referer</b> <i>ref_regexp</i>  <br><b>request-line</b> <i>req_regexp</i>  <br><b>user-agent</b> <i>ua_regexp</i> } |
| scr-ip       | Matches the source IP address and netmask of the request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>rule pattern-list</b> <i>list_num</i> <b>src-ip</b><br><i>s_ipaddress s_subnet</i>                                                                                                   |
| url-regex    | Matches the URL against a regular expression. The match is not case sensitive.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>rule pattern-list</b> <i>list_num</i><br><b>url-regex</b> <i>url_regexp</i>                                                                                                          |
| url-regsub   | <p>For the <b>rewrite</b> and <b>redirect</b> actions, matches the URL against a regular expression to form a new URL in accordance with the pattern substitution specification. The match is not case sensitive. The valid substitution index range is from 1 to 9.</p> <p><b>Note</b> For HTTP client requests for Windows Media Streaming live programs, an ASX file is created automatically; therefore, if you use the url-regsub pattern list to rewrite the filename from an .asf file extension to an .asx file extension, the SE is not able to find the file and returns a 404 error message.</p>                           | <b>rule pattern-list</b> <i>list_num</i><br><b>url-regsub</b> <i>url_regexp url_sub</i>                                                                                                 |

**Note**

A domain pattern list matching an SE IP address is not supported when IP-based redirection is enabled on the Service Router. See the “[Configuring the Service Router](#)” section on page 6-1 for more information about IP-based redirection. Flash Media Streaming bypasses the rules configuration if the request is from another SE.

**Step 8** Click **Submit** to save the settings.

**Tip**

The maximum number of pattern lists allowed is 128.

**Step 9** Associate an action with an existing pattern list:

- a. Choose an action type from the Rule Type drop-down list. See [Table 5-8](#) for a description of rule actions.
- b. In the Rule Parameters field, enter the list number of the pattern list that you want to associate with this action.

For example, if you want to block access by any protocol to yahoo.com, then choose **block** from the Rule Type drop-down list, and enter **pattern-list 72 protocol all** in the Rule Parameters field.



**Table 5-8**      **Service Rule Actions**

| Action Type            | Description                                                                                                                                                                                                                       | Syntax                                                                                                                                                                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| allow                  | Allows incoming requests that match the pattern list.<br>This rule action can be used in combination with block actions to allow selective types of requests. The allow action does not carry any meaning as a standalone action. | <b>rule action allow pattern-list</b><br><i>list_num</i> [protocol {all   http   rtmp   rtsp}]                                                                                                                                                             |
| block                  | Blocks this request and allows all others.                                                                                                                                                                                        | <b>rule action block pattern-list</b><br><i>list_num</i> [protocol {all   http   rtmp   rtsp}]                                                                                                                                                             |
| generate-url-signature | <b>Note</b> Not supported in Cisco ECDS 2.5.3 or 2.5.5.                                                                                                                                                                           | —                                                                                                                                                                                                                                                          |
| no-cache               | Does not cache this object.                                                                                                                                                                                                       | <b>rule action no-cache pattern-list</b><br><i>list_num</i> [protocol {all   http   rtmp   rtsp}]                                                                                                                                                          |
| redirect               | Redirects the original request to a specified URL. Redirect is relevant to the RADIUS server only if the RADIUS server has been configured for redirect.                                                                          | <b>rule action redirect url pattern-list</b><br><i>list_num</i> [protocol {all   http   rtmp   rtsp}]                                                                                                                                                      |
| refresh                | For a cache hit, forces an object freshness check with the server.                                                                                                                                                                | <b>rule action refresh pattern-list</b><br><i>list_num</i> [protocol {all   http}]                                                                                                                                                                         |
| replace                | Replace the text string in the object.                                                                                                                                                                                            | <b>rule action replace string_to_find string_to_replace pattern-list</b><br><i>list_num</i> [protocol {all   http   rtmp   rtsp}]                                                                                                                          |
| rewrite                | Rewrites the original request as a specified URL.                                                                                                                                                                                 | <b>rule action rewrite pattern-list</b><br><i>list_num</i> [protocol {all   http   rtmp   rtsp}]                                                                                                                                                           |
| validate-url-signature | <b>Note</b> Not supported in ECDS Release 2.5.3 through 2.5.5.                                                                                                                                                                    | <b>rule action validate-url-signature</b><br>{error-redirect-url url   exclude {all error-redirect-url url   client-ip error-redirect-url url   expiry-time error-redirect-url url} pattern-list<br><i>list_num</i> [protocol {all   http   rtmp   rtsp}]} |

- Step 10** Click **Submit** to save the settings.  
See [Enabling Apple HTTP Live Streaming](#).

## Enabling Apple HTTP Live Streaming

To enable a service rule to support Apple HTTP Live Streaming if you use it in your network:

- Step 1** Choose **Devices > Devices > Service Control > Service Rules**. The Service Rules Table page is displayed.
- Step 2** Click the **Create New** icon in the task bar. The Service Rules page is displayed ([Figure 5-8](#)).

- Step 3** From the **Rule Type** drop-down list, choose **pattern-list**.
- Step 4** In the **Rule Parameters** field, enter information using the guidelines shown on the Service Rules page (Table 5-7).
- Step 5** Use the following commands to enable the service rule to support Apple HLS:

```
SE(config)# rule enable
SE(config)# rule action no-cache pattern-list 20
SE(config)# rule pattern-list 20 url-regex .m3u8
SE(config)#
```

Figure 5-9 shows an example of configuring the rule type and parameters for Apple HTTP Live Streaming.

**Figure 5-9 Rule Type and Parameters - Apple HTTP Live Streaming**

Creating new Service Rules for Service Engine, cc-sre910-1

**Service Rules**

Rule Type:

Rule Parameters:

Rules Usage:

```
list-num domain dn_regex
list-num group-type {and | or}
list-num header-field {referer ref_regex | request-line req_regex | user-agent ua_regex}
list-num src-ip s_ipaddress s_subnet
list-num url-regex url_regex
list-num url-regsub url_regex url_sub
```

Note: \* - Required Field

Figure 5-10 shows an example of Apple HTTP Live Streaming configured in the Cisco ECDS GUI.

**Figure 5-10 Service Rules Settings - Apple HTTP Live Streaming**

Devices Services System

Devices Device Groups Locations Statistics

Expand All Show Basic Service Rules for Service Engine, wa-te1-se1 Rows: ALL

Aggregate Settings: ☒ Yes ☐ No

| Service Rule       | Device Group Source | Type         |
|--------------------|---------------------|--------------|
| 20 url-regex .m3u8 |                     | pattern-list |
| pattern-list 20    |                     | no-cache     |

<< Page 1 >> Showing 1-2 of 2 Service Rules

Device Home  
Device Activation  
Assignments  
Replication  
Request Routing  
Service Control  
Enable Rules  
Service Rules  
ICAP  
ICAP Services  
PCMM QoS Policy  
URL Signing  
Authorization Service  
Transaction Logging  
Application Control  
General Settings  
Monitoring

## Executing Rule Actions in Order

The order in which the rule actions are executed is different between the Web Engine and the other protocol engines (Windows Media Streaming, Movie Streamer, and Flash Media Streaming).

- [Web Engine Rule Action Order, page 5-17](#)
- [All Other Protocol Engine Rule Action Order, page 5-17](#)

**Note**

When configuring service rules, you must configure the same service rules on all SEs participating in a delivery service in order for the service rules to be fully implemented. The rule action must be common for all client requests because the SR may redirect a client request to any SE in a delivery service depending on threshold conditions.

### Web Engine Rule Action Order

The order in which the rule actions are executed for the Web Engine is as follows:

1. block or allow

**Note**

The allow and block actions carry the same precedence. The order of execution depends on the order of configuration between allow and block actions. Other actions always take precedence over allow.

2. redirect (before cache lookup)
3. rewrite (before cache lookup)
4. generate-url-signature
5. validate-url-signature
6. refresh (after cache lookup, in the case of cache hit)
7. no-cache

### All Other Protocol Engine Rule Action Order

The order in which the rule actions are executed for the other protocol engines is the order in which they were configured, except for the validate-url-signature action. If the rule pattern associated with the validate-url-signature action is matched, regardless of the configuration order the rules, the validate-url-signature action is performed before any other action.

1. validate-url-signature
2. block or allow

**Note**

The allow and block actions carry the same precedence. The order of execution depends on the order of configuration between allow and block actions. Other actions always take precedence over allow.

3. redirect (before cache lookup)
4. rewrite (before cache lookup)

## Configuring ICAP Services

The Internet Content Adaptation Protocol (ICAP) is not supported.

## Configuring PCMM QoS Policy

PCMM QoS Policy is not supported in this release.

## Configuring URL Signing

URL Signing is not supported in this release.

## Configuring the Authorization Service

When Authorization Service is enabled, client requests are blocked if the request is for an unknown server or if the client's IP address is not allowed to request content. The Authorization Service is enabled by default and includes both types of blocking.

The Authorization Service verifies that all client requests have a router fully qualified domain name (RFQDN) or origin server that is recognized as part of a delivery service. For more information about RFQDNs and origin server, see the [“Content Origins” section on page 8-1](#). If you want to allow client requests for unknown hosts, check the **Enable Unknown-Server Requests** check box.

Each delivery service participating in the Authorization Service has an XML configuration file that contains information on the allowed client IP addresses and geographic locations and denied client IP addresses and geographic locations. The Authorization Service blocks client requests based on the XML configuration file uploaded for the delivery service.

The SE that receives the client request compares the client's information, as well as the URL string pattern, with the information configured for the delivery service and allows or denies the request. If the Authorization Service denies the request, the protocol engine receives the denied message and sends a request denied message to the client. For more information, see the [“Configure Authorization Service” section on page 8-8](#).

To enable the Authorization Service:

---

**Step 1** Choose **Devices > Devices > Service Control > Authorization Service**. The Authorization Service page is displayed.

**Step 2** To enable the Authorization Service, check the **Enable Authorization** check box.



**Tip**

---

The Authorization Service is enabled by default.

---

**Step 3** To allow client requests for unknown hosts, while at the same time keeping the Authorization Service enabled, check the **Enable Unknown-Server Requests** check box.

**Step 4** Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

---

## Configuring Transaction Logging

Transaction logs allow administrators to view the traffic that has passed through the SE. Typical fields in the transaction log are the date and time when a request was made, the URL that was requested, whether it was a cache hit or a cache miss, the type of request, the number of bytes transferred, and the source IP address. For more information about transaction logs and their formats, see the [“Managing Transaction Logs” section on page 10-41](#).

To enable transaction logging:

- Step 1** Choose **Devices > Devices > Service Control > Transaction Logging**. The Transaction Log Settings page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 5-9](#) for a description of the fields.

**Table 5-9 Transaction Log Settings Fields**

| Field                                | Description                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General Settings</b>              |                                                                                                                                                                                                                                                                                                                                                                                       |
| Transaction Log Enable               | Enables transaction logging.                                                                                                                                                                                                                                                                                                                                                          |
| Log Windows Domain                   | If NTLM authentication is configured, you can record the Windows domain name and username in the “authenticated username” field of the transaction log by checking this check box. For more information, see the <a href="#">“Transaction Logging and NTLM Authentication” section on page 10-44</a> .                                                                                |
| Compress Files before Export         | When this check box is checked, archived log files are compressed into gzip format before being exported to external FTP servers                                                                                                                                                                                                                                                      |
| Log File Format<br>Log Format Custom | Log file format choices are <b>extended-squid</b> or <b>apache</b> . The default is <b>apache</b> . For more information, see the <a href="#">“Transaction Log Formats for Web Engine” section on page 10-42</a> .<br><br>Or, choose <b>Log Format Custom</b> and enter a custom format string. For more information, see the <a href="#">“Custom Format” section on page 10-43</a> . |
| <b>Archive Settings</b>              |                                                                                                                                                                                                                                                                                                                                                                                       |
| Max size of Archive File             | Maximum size (in kilobytes) of the archive file to be maintained on the local disk. The range is from 1000 to 2000000. The default is 500000.                                                                                                                                                                                                                                         |
| Max number of files to be archived   | Maximum number of files to be maintained on the local disk. The range is from 1 to 10000. The default is 10.                                                                                                                                                                                                                                                                          |

**Table 5-9 Transaction Log Settings Fields (continued)**

| Field                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Archive occurs         | <p>How often the working log is archived and the data is cleared from the working log. Choose one of the following:</p> <ul style="list-style-type: none"> <li>Choose <b>every</b> to archive every so many seconds, and enter the number of seconds for the interval. The range is from 120 to 604800.</li> <li>Choose <b>every hour</b> to archive using intervals of one hour or less, and choose one of the following: <ul style="list-style-type: none"> <li><b>at</b>—Specifies the minute in which each hourly archive occurs</li> <li><b>every</b>—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30)</li> </ul> </li> <li>Choose <b>every day</b> to archive using intervals of one day or less, and choose one of the following: <ul style="list-style-type: none"> <li><b>at</b>—Specifies the hour in which each daily archive occurs</li> <li><b>every</b>—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24)</li> </ul> </li> <li>Choose <b>every week on</b> to archive at intervals of one or more times a week, choose the days of the week, and choose what time each day.</li> </ul>  |
| <b>Export Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Enable Export          | Enables exporting of the transaction log to an FTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Export occurs          | <p>How often the working log is sent to the FTP server and the data is cleared from the working log. Choose one of the following:</p> <ul style="list-style-type: none"> <li>Choose <b>every</b> to export every so many minutes, and enter the number of minutes for the interval. The range is from 1 to 10080.</li> <li>Choose <b>every hour</b> to export using intervals of one hour or less, and choose one of the following: <ul style="list-style-type: none"> <li><b>at</b>—Specifies the minute in which each hourly export occurs</li> <li><b>every</b>—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30)</li> </ul> </li> <li>Choose <b>every day</b> to export using intervals of one day or less, and choose one of the following: <ul style="list-style-type: none"> <li><b>at</b>—Specifies the hour in which each daily export occurs</li> <li><b>every</b>—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24)</li> </ul> </li> <li>Choose <b>every week on</b> to export using intervals of one or more times a week, choose the days of the week, and what time each day.</li> </ul> |
| FTP Export Server      | IP address or hostname of the FTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Name                   | Name of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Password               | Password for the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Table 5-9 Transaction Log Settings Fields (continued)**

| Field                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Confirm Password              | Confirms the password for the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Directory                     | Name of the directory used to store the transaction logs on the FTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SFTP                          | Check the <b>SFTP</b> check box, if you are using an SFTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Windows Media Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Enable Windows Media Settings | Enables Windows Media transaction logging.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Log File Format               | <p>Sets Windows Media Streaming Engine to generate transaction logs in the following formats:</p> <ul style="list-style-type: none"> <li> <b>extended wms-41</b> Uses the standard Windows Media Services 4.1 format to generate the transaction log and includes the following three additional fields in the transaction log: <ul style="list-style-type: none"> <li>SE_action (cache hit or cache miss)</li> <li>SE-bytes (number of bytes sent from the SE for a cache hit)</li> <li>username (username of the Windows Media request when NTLM, Negotiate, Digest, or basic authentication is used)</li> </ul> </li> <li> <b>extended wms-90</b> Uses the standard Windows Media Services 9 format to generate the transaction log and includes the following three additional fields in the transaction log: <ul style="list-style-type: none"> <li>SE_action (cache hit or cache miss)</li> <li>SE-bytes (number of bytes sent from the SE for a cache hit)</li> <li>username (username of the Windows Media request when NTLM, Negotiate, Digest, or basic authentication is used)</li> </ul> </li> <li><b>wms-41</b> Standard Windows Media Services 4.1 format</li> <li><b>wms-90</b> Standard Windows Media Services 9 format</li> </ul> <p>The default is <b>wms-41</b>. For more information, see the <a href="#">“Windows Media Transaction Logging”</a> section on page 10-47.</p> |

**Step 3** Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

# Application Control

The Application Control pages provide settings for bandwidth management of delivery services and protocol engines. Configuring application control consists of the following procedures:

- [Configuring Bandwidth, page 5-22](#)
- [Configuring Windows Media Streaming, page 5-25](#)
- [Configuring Movie Streamer General Settings, page 5-35](#)
- [Configuring RTSP Advanced Settings, page 5-37](#)
- [Configuring Flash Media Streaming, page 5-37](#)
- [Configuring HTTP, page 5-39](#)
- [Configuring HTTPS, page 5-48](#)

## Configuring Bandwidth

- [Configuring Default and Maximum Bandwidth, page 5-22](#)
- [Configuring Bandwidth Schedules, page 5-23](#)
- [Bandwidth Graph, page 5-24](#)

### Configuring Default and Maximum Bandwidth

The bandwidth used for delivering content is determined by the settings in the Default and Maximum Bandwidth page, and the Scheduled Bandwidth page. The default settings are used unless a scheduled bandwidth is configured for a specified time period. For Flash Media Streaming bandwidth limits, see the “[Configuring Flash Media Streaming](#)” section on [page 5-37](#).

**Note**

The bandwidth used for delivering content is always the minimum bandwidth configured of the following configurations: default bandwidth, maximum bandwidth, and scheduled bandwidth. When the bandwidth limit is reached, new client requests are dropped and a syslog entry is written. The client receives an error message “453: Not enough bandwidth.”

See the following sections:

- [Configuring Bandwidth Schedules, page 5-23](#)
- [Bandwidth Graph, page 5-24](#)

**Procedure**

To configure the default and maximum bandwidth settings:

- Step 1** Choose **Devices > Devices > Application Control > Default and Maximum Bandwidth**. The Default and Maximum Bandwidth page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 5-10](#) for a description of the fields.



**Table 5-10 Application Control Default and Maximum Bandwidth Fields**

| Field                   |                   | Description                                                                                                                                                                                                                                                                             |
|-------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows Media Incoming  | Default Bandwidth | Default bandwidth allowed for incoming Windows Media traffic from client devices.                                                                                                                                                                                                       |
|                         | Maximum Bandwidth | Maximum bandwidth permitted by system license. The maximum bandwidth for concurrent Windows Media streams enforces the aggregate bandwidth of all concurrent Windows Media streaming sessions, which includes RTSP-using-UDP, RTSP-using-TCP, MMS-over-HTTP, and live stream splitting. |
| Windows Media Outgoing  | Default Bandwidth | Default bandwidth allowed for outgoing Windows Media traffic from the SE.                                                                                                                                                                                                               |
|                         | Maximum Bandwidth | Maximum bandwidth permitted by system license. The maximum bandwidth for concurrent Windows Media streams enforces the aggregate bandwidth of all concurrent Windows Media streaming sessions, which includes RTSP-using-UDP, RTSP-using-TCP, MMS-over-HTTP, and live stream splitting. |
| Movie Streamer Incoming | Default Bandwidth | Default bandwidth allowed for incoming Movie Streamer traffic from client devices.                                                                                                                                                                                                      |
|                         | Maximum Bandwidth | Maximum bandwidth permitted by system license. The maximum bandwidth for concurrent Movie Streamer streams enforces the aggregate bandwidth of all concurrent Movie Streamer sessions.                                                                                                  |
| Movie Streamer Outgoing | Default Bandwidth | Default bandwidth allowed for outgoing Movie Streamer traffic from the SE.                                                                                                                                                                                                              |
|                         | Maximum Bandwidth | Maximum bandwidth permitted by system license. The maximum bandwidth for concurrent Movie Streamer streams enforces the aggregate bandwidth of all concurrent Movie Streamer sessions.                                                                                                  |

**Step 3** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring Bandwidth Schedules

Bandwidth Schedule settings take precedence over Default Bandwidth settings.

To configure a Bandwidth Schedule:

- Step 1** Choose **Devices > Devices > Application Control > Bandwidth Schedules**. The Application Control Bandwidth Schedule Table page is displayed.
- The table is sortable by clicking the column headings.
- For information about Aggregate Settings, see the [“Managing Aggregate Settings” section on page 4-8](#)
- Step 2** Click **Create New** in the task bar. The Scheduled Bandwidth page is displayed.
- To edit a bandwidth schedule, click the **Edit** icon next to the scheduled bandwidth you want to edit.

**Step 3** Enter the settings as appropriate. See [Table 5-11](#) for a description of the fields.

**Table 5-11 Application Control Bandwidth Schedule Fields**

| Field              | Description                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bandwidth Type     | Windows Media Incoming—Incoming Windows Media streaming content requests from end users.<br>Windows Media Outgoing—Outgoing Windows Media content from SEs.<br>Movie Streamer Incoming—Incoming Movie Streamer content requests from SEs or origin servers.<br>Movie Streamer Outgoing—Outgoing Movie Streamer content in response to RTSP requests from end users. |
| Bandwidth Rate     | Maximum amount of bandwidth you want to allow (in kilobits per second).                                                                                                                                                                                                                                                                                             |
| Start Time         | Time of day for the bandwidth rate setting to start, using a 24-hour clock in local time (hh:mm).                                                                                                                                                                                                                                                                   |
| End Time           | Time of day for the bandwidth rate setting to end (hh:mm).                                                                                                                                                                                                                                                                                                          |
| Use Specific Days  | Days of the week on which configured bandwidth settings apply. <ul style="list-style-type: none"> <li>Full Week—Bandwidth settings are applied to the entire week.</li> <li>Sun, Mon, Tue, Wed, Thu, Fri, and Sat—Specific days of the week on which configured bandwidth settings apply.</li> </ul>                                                                |
| Specific Day Range | Range of days of the week on which configured bandwidth settings apply. <ul style="list-style-type: none"> <li>Start day—Day of the week to start for allowable bandwidth.</li> <li>End day—Day of the week to end for allowable bandwidth.</li> </ul>                                                                                                              |

**Step 4** Click **Submit** to save the settings.

To delete a bandwidth schedule, click the **Edit** icon for the group, then click the **Delete** icon in the task bar.

## Bandwidth Graph

To view a graphical representation of the bandwidth settings, click the **Display Graph** icon in the task bar. The Application Bandwidth graph is displayed in a new window.

The vertical axis of the graph represents the amount of bandwidth in kilobits per second (kb/s), and the horizontal axis represents the days of the week. The units shown on the vertical axis are determined dynamically based on the bandwidth rate for a particular bandwidth type. The units shown on the horizontal axis represent 24 hours per each day of the week. Each type of bandwidth is represented by a different color. A legend at the bottom of the graph maps colors to the corresponding bandwidth type.

To view the graph by bandwidth type, detailed or composite view, or days of the week, click a view option in the text at the top of the window. [Table 5-12](#) describes the view options.

**Table 5-12 Viewing Options for Content Services Bandwidth Graph**

| Option                                           | Description                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows Media In                                 | Displays the bandwidth settings for incoming Windows Media traffic.                                                                                                                                                                                                                                                                                                                                       |
| Windows Media Out                                | Displays the bandwidth settings for outgoing Windows Media traffic.                                                                                                                                                                                                                                                                                                                                       |
| Movie Streamer In                                | Displays the bandwidth settings for incoming Movie Streamer traffic.                                                                                                                                                                                                                                                                                                                                      |
| Movie Streamer Out                               | Displays the bandwidth settings for outgoing Movie Streamer traffic.                                                                                                                                                                                                                                                                                                                                      |
| All Servers                                      | Displays a consolidated view of all configured bandwidth types. This is the default view and is combined with the Full Week view.                                                                                                                                                                                                                                                                         |
| Show Detailed Bandwidth/Show Effective Bandwidth | <p>Toggles between the two options:</p> <p>Show Detailed Bandwidth—Displays detailed bandwidth settings for the SE and its associated device groups. The bandwidth settings of the device and device groups are shown in different colors for easy identification.</p> <p>Show Effective Bandwidth—Displays the composite (aggregate) bandwidth settings for the SE and its associated device groups.</p> |
| Show Aggregate View/Show Non-Aggregate View      | <p>Toggles between the two options:</p> <p>Show Aggregate View—Displays the bandwidth settings configured for the corresponding device groups.</p> <p>Show Non-Aggregate View—Displays the bandwidth settings configured for the SE.</p>                                                                                                                                                                  |
| Sun, Mon, Tues, Wed, Thurs, Fri, Sat             | Displays the bandwidth settings for the corresponding day of the week.                                                                                                                                                                                                                                                                                                                                    |
| Full Week                                        | Displays the bandwidth settings for the entire week. This is the default view and is combined with the All Servers view.                                                                                                                                                                                                                                                                                  |

## Configuring Windows Media Streaming

- [Configuring General Settings, page 5-26](#)
- [Configuring the Windows Media Outgoing Proxy Bypass List, page 5-32](#)
- [Configuring the Windows Media Outgoing Proxy Bypass List, page 5-32](#)
- [WMT Outgoing HTTP Proxy Bypass Commands, page 5-32](#)
- [Configuring the Outgoing RTSP Proxy Bypass List, page 5-33](#)
- [WMT Outgoing RTSP Proxy Bypass Commands, page 5-34](#)

## Configuring General Settings

To configure the General Settings for Windows Media Streaming:

- 
- Step 1** Choose **Devices > Devices > Application Control > Windows Media Streaming > General Settings**. The Windows Media Streaming General Settings page is displayed ([Figure 5-11](#)).

**Figure 5-11** *Windows Media Streaming Page—General Settings*

Expand All

Show Basic

Windows Media Settings for Service Engine, *gluon*

Device Home

Device Activation

Assignments

Replication

Request Routing

Service Control

Application Control

Default and Maximum Bandwidth

Bandwidth Schedules

Windows Media Streaming

General Settings

Bypass List

Movie Streamer

RTSP Advanced Settings

Flash Media Streaming

Web

General Settings

Monitoring

Windows Media Settings will be enabled when using Factory Defaults. The values shown in this page are in effect.

### Windows Media Settings

Current settings: None (Using Factory Defaults)

Enable Windows Media Services: ☒

### Windows Media Proxy Settings

Enable Outgoing HTTP Proxy: ☐ Host Name:  Port:

Outgoing HTTP Proxy Bypass Domains:  Space separated list of up to 32 Domains

Outgoing HTTP Proxy Bypass List:  Space separated list of up to 32 Addresses (entered in CIDR notation i.e. 10.10.10.10/24)

Enable Outgoing RTSP Proxy: ☐ Host Name:  Port:

Outgoing RTSP Proxy Bypass Domains:  Space separated list of up to 32 Domains

Outgoing RTSP Proxy Bypass List:  Space separated list of up to 32 Addresses (entered in CIDR notation i.e. 10.10.10.10/24)

Enable Accelerate Proxy Cache Performance: ☒

### Windows Media General Settings

Disable HTTP Windows Media Traffic: ☐ Disable RTSP WMT Traffic: ☐ Disable RTSPU WMT Traffic: ☐

Maximum Concurrent Connections:

Override default: ☐ Custom Value:  (1-14000) We recommend using default value, which optimizes performance based on hardware model and the applications you've enabled.

Enforce Maximum Outgoing Bitrate: ☐

Maximum Outgoing Bitrate:  (Kbps) (1-2147483647) The maximum value for outgoing bitrate depends on the hardware model.

Enforce Maximum Incoming Bitrate: ☐

Maximum Incoming Bitrate:  (Kbps) (1-2147483647) The maximum value for incoming bitrate depends on the hardware model.

Enable Accelerate Live-Split Performance: ☒

Enable Accelerate VOD Performance: ☒

Restrict HTTP Allowed Extensions: ☐

HTTP Allowed Extensions:  asf none nsc wma wmv ns Space separated list of extensions

Enable Fast Start Feature: ☒

Fast Start Max Bandwidth:  (kbps) (1-65535)

Enable Fast Cache: ☒

Fast Cache Max Delivery Rate:  per second (1-65535)

### Windows Media Multicast Settings

Number of hops to live:  (0-255)

### Windows Media Advanced Client Settings

Idle Timeout:  (seconds) (30-300)

Maximum data packet size:  (bytes) (576-16000)

### Windows Media Advanced Server Settings

Enable Log Forwarding: ☒

Inactive Timeout:  (seconds) (60-65535)

### Windows Media Cache Settings

Enable: ☒

Max Object Size:  (MB) (1-1000000)

Age Multiplier:  % (0-100)

Maximum TTL:  days

Minimum TTL:  (Minutes) (0-86400)

Enable Re-evaluate Request: ☐

**Step 2** Enter the settings as appropriate. See [Table 5-13](#) for a description of the fields.

**Table 5-13 Windows Media Streaming General Settings Fields**

| Field                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Windows Media Services          | When checked, Windows Media Services is enabled. To disable services, uncheck the check box.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Windows Media Proxy Settings</b>    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Enable Outgoing HTTP Proxy             | When enabled, allows an outgoing HTTP proxy server for streaming media in MMS format (MMS-over-HTTP). The Outgoing Proxy feature only works on the Content Acquirer in a delivery service.                                                                                                                                                                                                                                                                                                                                                   |
| Outgoing HTTP Proxy Host Name and Port | Hostname, or IP address, and port of the outgoing HTTP proxy. Valid port numbers range from 1 to 65535.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Outgoing HTTP Proxy Bypass Domains     | <p>If an incoming MMS over HTTP request matches a domain configured in this list, it will not be forwarded to the configured HTTP proxy server. The request will be routed according to its destination FQDN.</p> <p>This field is activated when you select the Enable Outgoing HTTP Proxy check box. Separate up to 32 outgoing proxy domain entries with a space.</p> <p>See the <a href="#">“Configuring Proxy Bypass Lists”</a> section on page 5-32.</p>                                                                               |
| Outgoing HTTP Proxy Bypass List        | <p>If an incoming MMS over HTTP request matches the IP address or subnet configured in this list, it will not be forwarded to the configured HTTP proxy server. The request will be routed according to its destination IP address.</p> <p>This field is activated when you select the Enable Outgoing HTTP Proxy check box. Separate up to 32 outgoing proxy bypass addresses with a space (entered in CIDR notation, for example 10.10.10.10/24).</p> <p>See the <a href="#">“Configuring Proxy Bypass Lists”</a> section on page 5-32</p> |
| Enable Outgoing RTSP Proxy             | When enabled, allows an outgoing RTSP proxy server for streaming media using RTSP. The Outgoing Proxy feature only works on the Content Acquirer in a delivery service.                                                                                                                                                                                                                                                                                                                                                                      |
| Outgoing RTSP Proxy Bypass Domains     | <p>If an incoming WMT RTSP request matches a domain configured in this list, it will not be forwarded to the configured RTSP proxy server. The request will be routed according to its destination FQDN.</p> <p>This field is activated when you select the Enable Outgoing HTTP Proxy check box. Separate up to 32 outgoing proxy domain entries with a space.</p> <p>See the <a href="#">“Configuring Proxy Bypass Lists”</a> section on page 5-32.</p>                                                                                    |

**Table 5-13 Windows Media Streaming General Settings Fields (continued)**

| Field                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Outgoing RTSP Proxy Bypass List                                   | <p>If an incoming WMT RTSP request matches the IP address or subnet configured in this list, it will not be forwarded to the configured RTSP proxy server. The request will be routed according to its destination IP address.</p> <p>This field is activated when you select the Enable Outgoing HTTP Proxy check box. Separate up to 32 outgoing proxy bypass addresses with a space (entered in CIDR notation, for example 10.10.10.10/24).</p> <p>See the <a href="#">“Configuring Proxy Bypass Lists”</a> section on page 5-32.</p> |
| Outgoing RTSP Proxy Host Name and Port                            | Hostname, or IP address, and port of the outgoing RTSP proxy. Valid port numbers range from 1 to 65535.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Enable Accelerate Proxy Cache Performance                         | When enabled, caching performance improvements are applied to the Windows Media proxy.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Windows Media General Settings</b>                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Disable HTTP Windows Media Traffic                                | To disallow streaming over HTTP, check the check box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Disable RTSPT WMT Traffic                                         | To disallow streaming over RTSPT (RTSP using TCP), check the check box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Disable RTSPU WMT Traffic                                         | To disallow streaming over RTSPU (RTSP using UDP), check the check box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Maximum Concurrent Connections: Override Default and Custom Value | To override the default maximum number of concurrent sessions, check the check box and enter a value in the <b>Custom Value</b> field. The default is 14000 sessions. The range is from 1 to 14000.                                                                                                                                                                                                                                                                                                                                      |
| Enforce Maximum Outgoing Bitrate                                  | Enforces the maximum stream bit rate for serving content when checked.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Maximum Outgoing Bitrate                                          | The maximum streaming bit rate that can be served in kilobits per second (kbps).                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Enforce Maximum Incoming Bitrate                                  | Enforces the maximum incoming bit rate for receiving content when checked.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Maximum Incoming Bitrate                                          | The maximum streaming bit rate (kbps) that can be received.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Enable Accelerate Live-Split Performance                          | Enables performance improvements in live splitting for the Windows Media proxy.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Enable Accelerate VOD Performance                                 | Enables performance improvements in Video On Demand for the Windows Media proxy.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Restrict HTTP Allowed Extensions                                  | Allows you to add or remove permitted extensions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Table 5-13 Windows Media Streaming General Settings Fields (continued)**

| Field                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP Allowed Extensions                       | <p>List of allowable extensions for HTTP.</p> <p>You can add or delete filename extensions from this list with the following restrictions:</p> <ul style="list-style-type: none"> <li>Each extension must be alphanumeric, with the first character in the extension being an alphabetic character.</li> <li>You cannot have more than 10 characters in a filename extension.</li> <li>You cannot add more than 6 filename extensions to the allowed list.</li> </ul> |
| Enable Fast Start Feature                     | Enables Fast Start for MMS-over-HTTP or RTSP.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Fast Start Max Bandwidth                      | Maximum bandwidth (kbps) allowed per Windows Media Player when Fast Start is used to serve packets to this player. The default is 3500. The range is from 1 to 65535.                                                                                                                                                                                                                                                                                                 |
| Enable Fast Cache                             | Enables Fast Cache for MMS-over-HTTP or RTSP.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Fast Cache Max Delivery Rate                  | Maximum delivery rate (kbps) allowed per Windows Media Player when Fast Cache is used to deliver packets to this player. The default is 5. The range is from 1 to 65535.                                                                                                                                                                                                                                                                                              |
| <b>Windows Media Multicast Settings</b>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Number of hops to live                        | Number of hops to live for multicast Windows Media packets. The default is 5. The range is from 0 to 255.                                                                                                                                                                                                                                                                                                                                                             |
| <b>Windows Media Advanced Client Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Idle Timeout                                  | Number of seconds to timeout when the client connection is idle. The default is 60. The range is from 30 to 300.                                                                                                                                                                                                                                                                                                                                                      |
| Maximum Data Packet Size                      | Maximum packet size (in bytes) allowed. The default is 1500. The range is from 576 to 16,000.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Windows Media Advanced Server Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Enable Log Forwarding                         | Enables log forwarding to an upstream SE or Windows Media server.                                                                                                                                                                                                                                                                                                                                                                                                     |
| Inactive Timeout                              | Number of seconds to timeout when the upstream SE or Windows Media server connection is idle. The default is 65535. The range is from 60 to 65535.                                                                                                                                                                                                                                                                                                                    |
| <b>Windows Media Cache Settings</b>           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Enable                                        | When checked, Windows Media cache settings are enabled.                                                                                                                                                                                                                                                                                                                                                                                                               |
| Max Object Size                               | The maximum content object size (in megabytes) the SE can cache. The default is 25600. The range is from 1 to 10000000.                                                                                                                                                                                                                                                                                                                                               |
| Age Multiplier                                | The age multiplier value (as a percentage) enables the SE to estimate the life of an object by multiplying the time since the object was last modified by a percentage to obtain an approximate expiration date. After this date, the object is considered stale, and subsequent results cause a fresh retrieval by the SE. The default value is 30. The range is from 0 to 100.                                                                                      |



**Table 5-13** Windows Media Streaming General Settings Fields (continued)

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum TTL                | The maximum time-to-live for objects in the cache. The value ranges are the following:<br>1 to 157680000 seconds<br>1 to 2628000 minutes<br>1 to 43800 hours<br>1 to 1825 days<br>The default is 1 day.                                                                                                                                                      |
| Minimum TTL                | The minimum time-to-live (in minutes) for objects in the cache. The default is 60. The range is from 0 to 86400.                                                                                                                                                                                                                                             |
| Enable Re-evaluate Request | When checked, the cache is validated with the origin server instead of validating the cache using heuristics. When Enable Re-evaluate Request is checked, the cached content freshness is revalidated every time the content is requested, which limits the effectiveness of the other cache settings and increases the time to start streaming the content. |

**Step 3** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring the Incoming Bandwidth Bypass List

Incoming bandwidth refers to the bandwidth between a local SE and the origin server. When the SE is configured for Windows Media proxy services, incoming bandwidth usage for Video On Demand (VOD) content is unpredictable because the consumption of incoming bandwidth for VOD content can be triggered arbitrarily by an end user requesting the content. If the VOD content is not found in the SE cache, a cache miss occurs, and the Windows Media proxy must fetch the content from the origin server. The SE administrator cannot predict the incoming bandwidth usage for such events, so a large number of cache-miss VOD requests can consume all of the incoming bandwidth.

The Windows Media incoming bandwidth bypass configuration allows the administrator to configure a list of hosts that bypasses the incoming bandwidth limitation.

To configure the list of hosts for bypassing incoming bandwidth limits:

- Step 1** Choose **Devices > Devices > Application Control > Windows Media Streaming > Bypass List**. The Bypass List page is displayed.
- Step 2** In the **Windows Media BW Incoming Bypass List** field, enter up to four IP addresses or hostnames of hosts you want to bypass the incoming bandwidth check. Separate each entry with a space.
- Step 3** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring Proxy Bypass Lists

- [Configuring the Windows Media Outgoing Proxy Bypass List, page 5-32](#)
- [Configuring the Windows Media Outgoing Proxy Bypass List, page 5-32](#)
- [WMT Outgoing HTTP Proxy Bypass Commands, page 5-32](#)
- [Configuring the Outgoing RTSP Proxy Bypass List, page 5-33](#)
- [WMT Outgoing RTSP Proxy Bypass Commands, page 5-34](#)

### Configuring the Windows Media Outgoing Proxy Bypass List

The bypass function allows a service engine to skip the forwarding of some WMT requests to the proxy bypass server based on destination domain or IP address.

To configure the Outgoing HTTP Proxy Bypass list:

- Step 1** Choose **Devices > Devices > Application Control > Windows Media Streaming > General Settings**.
- Step 2** Select the **Enable Outgoing HTTP Proxy** check box. The Outgoing HTTP Proxy fields become active, as shown in [Figure 5-12](#).

**Figure 5-12** Enabling Outgoing HTTP Proxy

Enable Outgoing HTTP Proxy: ☒ Host Name: \*  Port: \*

Outgoing HTTP Proxy Bypass Domains:  Space separated list of up to 32 Domains

Outgoing HTTP Proxy Bypass List:  Space separated list of up to 32 Addresses (entered in CIDR notation i.e. 10.10.10.10/24)

- Step 3** Enter either domains or IP addresses to be bypassed by the outgoing HTTP proxy in the Outgoing HTTP Proxy Bypass Domains textbox or Outgoing HTTP Proxy Bypass List textbox, respectively. Each entry is separated by a single space.
- List of domains: Domain entries can be either a fully qualified domain name or a general domain. For example, a FQDN entry of `ecds.cisco.com` will bypass proxying of all requests intended for that server. An entry of `cisco.com` will bypass all sub-domains within `cisco.com`, including `ecds.cisco.com`.
  - List of subnets/IP addresses: Subnets and IP addresses should be entered in CIDR notation. For example, the subnet `10.10.10.0` should be entered in the form `10.10.10.0/24`. Single IP addresses will also need to be in CIDR notation, with 32 as the CIDR subnet suffix. For example, the IP address `10.10.10.10` should be entered in the form `10.10.10.10/32`.

To configure outgoing HTTP proxy bypass list using CLI, proceed to the [“WMT Outgoing HTTP Proxy Bypass Commands” section on page 5-32](#).

### WMT Outgoing HTTP Proxy Bypass Commands

- Step 1** To add a domain to the outgoing HTTP proxy bypass list, enter the following command:

```
SE(config)# wmt proxy outgoing http bypass domain-name [domain]
```

Multiple domains can be added to the outgoing HTTP proxy bypass list using the follow format:

```
SE(config)# wmt proxy outgoing http bypass domain-name [domain 1] [domain 2]...
```

Up to 32 domains can be entered.

- Step 2** To remove a domain from the outgoing HTTP proxy bypass list, enter the following command:

```
SE(config)# no wmt proxy outgoing http bypass domain-name [domain 1] [domain 2]...
```

Multiple domains can be removed at a time.

- Step 3** To add a single IP address to the outgoing HTTP proxy bypass list, enter the following command:

```
SE(config)# wmt proxy outgoing http bypass ip-address [IP-address] subnet-mask
255.255.255.255
```

- Step 4** To add a subnet to the outgoing HTTP proxy bypass list, enter the following command:

```
SE(config)# wmt proxy outgoing http bypass ip-address [IP-address] subnet-mask [Netmask]
```



**Note** The mask address is not in CIDR notation, and will be in standard IP mask notation, for example 255.255.255.0

- Step 5** To remove an IP address or subnet from the outgoing HTTP proxy bypass list, enter the following command:

```
SE(config)# no wmt proxy outgoing http bypass ip-address [IP-address] subnet-mask
[Netmask]
```

## Configuring the Outgoing RTSP Proxy Bypass List

To configure the Outgoing RTSP Proxy Bypass list:

- Step 1** Choose **Devices > Devices > Application Control > Windows Media Streaming > General Settings**.
- Step 2** Select the **Enable Outgoing RTSP Proxy** check box. The Outgoing RTSP Proxy fields become active, as shown in [Figure 5-13](#).

**Figure 5-13** RTSP Proxy Bypass List

| Windows Media Proxy Settings               |                                                                                                                                             |             |                                          |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------------|
| Enable Outgoing HTTP Proxy:                | <input type="checkbox"/>                                                                                                                    | Host Name:* | <input type="text"/>                     |
|                                            |                                                                                                                                             | Port:*      | <input type="text"/>                     |
| Outgoing HTTP Proxy Bypass Domains:        | <input type="text"/> Space separated list of up to 32 Domains                                                                               |             |                                          |
| Outgoing HTTP Proxy Bypass List:           | <input type="text"/> Space separated list of up to 32 Addresses (entered in CIDR notation i.e. 10.10.10/24)                                 |             |                                          |
| Enable Outgoing RTSP Proxy:                | <input checked="" type="checkbox"/>                                                                                                         | Host Name:* | <input type="text" value="10.10.10.10"/> |
|                                            |                                                                                                                                             | Port:*      | <input type="text" value="9000"/>        |
| Outgoing RTSP Proxy Bypass Domains:        | <input type="text" value="cisco.com california.com"/> Space separated list of up to 32 Domains                                              |             |                                          |
| Outgoing RTSP Proxy Bypass List:           | <input type="text" value="11.1.1.0/24 12.2.3.4/32"/> Space separated list of up to 32 Addresses (entered in CIDR notation i.e. 10.10.10/24) |             |                                          |
| Enable Accelerate Proxy Cache Performance: | <input checked="" type="checkbox"/>                                                                                                         |             |                                          |

- Step 3** Enter either domains or IP addresses to be bypassed by the outgoing HTTP proxy in the Outgoing RTSP Proxy Bypass Domains textbox or Outgoing RTSP Proxy Bypass List textbox, respectively. Each entry is separated by a single space.
- List of domains: Domain entries can be either a fully qualified domain name or a general domain. For example, a FQDN entry of `ecds.cisco.com` will bypass proxying of all requests intended for that server. An entry of `cisco.com` will bypass all sub-domains within `cisco.com`, including `ecds.cisco.com`.
  - List of subnets/IP addresses: Subnets and IP addresses should be entered in CIDR notation. For example, the subnet `10.10.10.0` should be entered in the form `10.10.10.0/24`. Single IP addresses will also need to be in CIDR notation, with 32 as the CIDR subnet suffix. For example, the IP address `10.10.10.10` should be entered in the form `10.10.10.10/32`.

To configure outgoing RTSP proxy bypass list using CLI, proceed to the [“WMT Outgoing RTSP Proxy Bypass Commands” section on page 5-34](#).

## WMT Outgoing RTSP Proxy Bypass Commands

- Step 1** To add a domain to the outgoing RTSP proxy bypass list, enter the following command:

```
SE(config)# wmt proxy outgoing rtsp bypass domain-name [domain]
```

Multiple domains can be added to the outgoing RTSP proxy bypass list using the follow format:

```
SE(config)# wmt proxy outgoing rtsp bypass domain-name [domain 1] [domain 2]...
```

Up to 32 domains can be entered.

- Step 2** To remove a domain from the outgoing RTSP proxy bypass list, enter the following command:

```
SE(config)# no wmt proxy outgoing rtsp bypass domain-name [domain 1] [domain 2]...
```

Multiple domains can be removed at a time.

- Step 3** To add a single IP address to the outgoing RTSP proxy bypass list, enter the following command:

```
SE(config)# wmt proxy outgoing rtsp bypass ip-address [IP-address] subnet-mask
255.255.255.255
```

- Step 4** To add a subnet to the outgoing RTSP proxy bypass list, enter the following command:

```
SE(config)# wmt proxy outgoing rtsp bypass ip-address [IP-address] subnet-mask [Netmask]
```



**Note** The mask address is not in CIDR notation, and will be in standard IP mask notation, for example `255.255.255.0`.

- Step 5** To remove an IP address or subnet from the outgoing RTSP proxy bypass list, enter the following command:

```
SE(config)# no wmt proxy outgoing rtsp bypass ip-address [IP-address] subnet-mask
[Netmask]
```

## Configuring Movie Streamer General Settings

The Movie Streamer is an open-source, standards-based, streaming server that delivers hinted MPEG-4, hinted 3GPP, and hinted MOV files to clients over the Internet and mobile networks using the industry-standard RTP and RTSP.

To configure the general settings for Movie Streamer:

- Step 1** Choose **Devices > Devices > Application Control > Movie Streamer > General Settings**. The Movie Streamer General Settings page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 5-14](#) for a description of the fields.

**Table 5-14** *Movie Streamer General Settings Fields*

| Field                                                             | Description                                                                                                                                                                                        |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Movie Streamer Services                                    | When checked, Movie Streamer Services is enabled. To disable services, uncheck the check box.                                                                                                      |
| <b>Movie Streamer Proxy Settings</b>                              |                                                                                                                                                                                                    |
| Host Name                                                         | Hostname or IP address of the proxy server for Movie Streamer.                                                                                                                                     |
| Port                                                              | Port of the proxy server for Movie Streamer. Valid port numbers range from 1 to 65535. The default is 554.                                                                                         |
| <b>Movie Streamer General Settings</b>                            |                                                                                                                                                                                                    |
| Maximum Concurrent Connections: Override Default and Custom Value | To override the default maximum number of concurrent sessions, check the check box and enter a value in the <b>Custom Value</b> field. The default is 8000 sessions. The range is from 1 to 16000. |
| Enforce Maximum Outgoing Bitrate                                  | Enforces the maximum stream bit rate for serving content when checked.                                                                                                                             |
| Maximum Outgoing Bitrate                                          | The maximum streaming bit rate that can be served in kilobytes per second (Kbps).                                                                                                                  |
| Enforce Maximum Incoming Bitrate                                  | Enforces the maximum incoming bit rate for receiving content when checked.                                                                                                                         |
| Maximum Incoming Bitrate                                          | The maximum streaming bit rate (Kbps) that can be received.                                                                                                                                        |
| Enable Accelerate VOD Performance                                 | Enables performance improvements in Video On Demand for the Movie Streamer proxy.                                                                                                                  |

**Table 5-14** *Movie Streamer General Settings Fields (continued)*

| Field                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Movie Streamer Advanced Client Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Idle Timeout                                   | <p>The Idle Timeout field and the <b>movie-streamer advanced client idle-timeout</b> command (as well as the <b>movie-streamer advanced client rtp-timeout</b> command), are only intended for performance testing when using certain testing tools that do not have full support of the RTCP receiver report. Setting these timeouts to high values causes inefficient tear-down of client connections when the streaming sessions have ended.</p> <p>The <b>movie-streamer advanced client idle-timeout</b> command has a range from 0 to 300, whereas the <b>Idle Timeout</b> field has a range from 30-180. This is by design.</p> <p>For typical deployments, it is preferable to leave these parameters set to their defaults. The default is 60.</p> |
| <b>Movie Streamer Cache Settings</b>           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Enable                                         | When checked, Movie Streamer caches content on the SE and the cache settings are enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Age Multiplier                                 | The age multiplier value (as a percentage) enables the SE to estimate the life of an object by multiplying the time since the object was last modified by a percentage to obtain an approximate expiration date. After this date, the object is considered stale, and subsequent results cause a fresh retrieval by the SE. The default value is 30. The range is from 0 to 100.                                                                                                                                                                                                                                                                                                                                                                            |
| Maximum TTL                                    | <p>The maximum time-to-live for objects in the cache. The value ranges are the following:</p> <p>1 to 157680000 seconds</p> <p>1 to 2628000 minutes</p> <p>1 to 43800 hours</p> <p>1 to 1825 days</p> <p>The default is 1 day.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Enable Re-evaluate Request                     | When checked, the cache is validated with the origin server instead of validating the cache using heuristics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Step 3** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring RTSP Advanced Settings

To configure RTSP advanced settings for the Movie Streamer:

- Step 1** Choose **Devices > Devices > Application Control > RTSP Advanced Settings**. The RTSP Advanced Settings page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 5-15](#) for a description of the fields.

**Table 5-15** RTSP Advanced Settings Fields

| Field                       | Description                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Maximum Initial Setup Delay | Maximum delay allowed (in seconds) between TCP accept and the first RTSP message from the client. The default is 10 seconds. |
| Maximum Request Rate        | Maximum number of incoming requests per second that the RTSP gateway allows. The default is 40 requests per second.          |

- Step 3** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring Flash Media Streaming

- [Configuring General Settings, page 5-37](#)
- [Configuring the FMS Administrator, page 5-38](#)
- [Configuring Flash Media Streaming Service Monitoring, page 5-39](#)

### Configuring General Settings

The Flash Media Streaming engine delivers Adobe Flash applications and video files, as well as MP3 audio files using HTTP. For more information, see the “[Flash Media Streaming Engine](#)” section on [page 1-16](#).



**Note**

Flash Media Streaming uses port 1935 for RTMP and RTMPE streaming.

To enable Flash Media Streaming:

- Step 1** Choose **Devices > Devices > Application Control > Flash Media Streaming > General Settings**. The Flash Media Streaming General Settings page is displayed.
- Step 2** Check the **Enable Flash Media Streaming** check box.
- Step 3** Enter the settings as appropriate. See [Table 5-16](#) for a description of the fields.

**Table 5-16**      *Flash Media Streaming Fields*

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Perpetual License Bandwidth  | Maximum bandwidth of the perpetual license. The range is from 1000 to 8000000 Kbps. The default is 200000.                                                                                                                                                                                                                                                                                                                                                                        |
| Restricted Maximum Bandwidth | Maximum bandwidth allowed for Flash Media Streaming. The range is from 1000 to 8000000 Kbps. The default is 200000.<br><br>For best results, set the following bandwidth allocations: <ul style="list-style-type: none"> <li>• # 2 port with port channel, limit is 2 gigabit—<br/>Use the <b>flash-media-streaming max-bandwidth 2000000</b> command.</li> <li>• #1 port, limit is 1 gigabit—<br/>Use the <b>flash-media-streaming max-bandwidth 1000000</b> command.</li> </ul> |
| Restricted Maximum Sessions  | Maximum concurrent sessions the Flash Media Streaming engine supports. The range is from 1 to 15000. The default is 200.                                                                                                                                                                                                                                                                                                                                                          |

**Step 4** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring the FMS Administrator

To enable servers to send Flash Media Server (FMS) Administration API calls to this device:

- Step 1** Choose **Devices > Devices > Application Control > Flash Media Streaming > FMS Admin Allow Hosts**. The FMS Admin Allow Hosts page is displayed.
- Step 2** Check the **Enable** check box.
- Step 3** In the **FMS Admin Allow Hosts** field, enter the IP addresses (space delimited) of the servers that are allowed to send Flash Media Server Administration API calls to this device.
- The Adobe Flash Media Server Administration APIs and the Administration Console that was built using the Administration APIs are supported. These APIs can be used to monitor and manage the Adobe Flash Media Server running on a Cisco ECDS Service Engine.
- Step 4** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.



## Configuring Flash Media Streaming Service Monitoring

To enable Flash Media Streaming Service Monitoring:

- 
- Step 1** Choose **Devices > Devices > Application Control > Flash Media Streaming > Service Monitoring**. The Service Monitoring page is displayed.
- Step 2** Check the **Enable Service Monitoring** check box.
- Service Monitoring monitors the Flash Media Streaming engine memory usage. If the memory usage reaches the 1.5 GB limit for either the Flash Media Streaming core process or the Flash Media Streaming edge process, an alarm is raised and the Service Router does not redirect any new Flash Media Streaming requests to this SE.
- Step 3** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Configuring HTTP

- [Configuring Web Engine HTTP Connections, page 5-39](#)
- [Configuring the Outgoing Proxy Bypass List, page 5-42](#)
- [Configuring Web Engine HTTP Caching, page 5-43](#)
- [Configuring Web Engine HTTP Cache Freshness, page 5-45](#)
- [Configuring Web Engine Advanced HTTP Caching, page 5-46](#)

## Configuring Web Engine HTTP Connections

To configure web engine HTTP connections:

- 
- Step 1** Choose **Devices > Devices > Application Control > Web > HTTP > HTTP Connections**. The HTTP Connections page is displayed.
- Step 2** Enter the settings as appropriate using the information in [Table 5-17](#) as a guide.

**Table 5-17 HTTP Connections Fields**

| Field                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web engine Maximum Concurrent Connections     | (Required) The maximum concurrent sessions the Web engine supports. The range is from 100 to 12,000. The default is 2000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Enable IP Spoofing                            | <p>When enabled on a WCCP v2 router, the Service Engine sends and receives packets transparently with the client IP and sends the packets to the waiting application so that the TCP connection is not broken.</p> <p>To enable, select the Enable IP Spoofing check box.</p> <p><b>Note</b> You must configure WCCP before you can enable IP Spoofing. Disable the IP Spoofing feature by unchecking the Enable IP Spoofing check box in the ECDS GUI before configuring WCCP.</p> <ol style="list-style-type: none"> <li>1. See the <a href="#">“Configuring WCCP General Settings”</a> section on page 7-1 to enable WCCP.</li> <li>2. For more information about IP Spoofing, see the <a href="#">“IP Spoofing for HTTP”</a> section on page 2-23 and <a href="#">“Configuring HTTP IP Spoofing with WCCP”</a> section on page 7-19.</li> </ol> |
| Enable Incoming Proxy                         | <p>When enabled, accepts incoming requests on configured ports, in addition to port 80.</p> <p><b>Note</b> Not supported for HTTPS in this release.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| List of Incoming HTTP Ports                   | <b>Note</b> Not used in this release.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Enable Outgoing Proxy                         | <p>When enabled, allows a proxy server or another SE to receive HTTP cache miss request traffic. The Outgoing Proxy feature only works on the Content Acquirer in a delivery service.</p> <p><b>Tip</b> When this box is checked, the Outgoing Proxy Authentication Fields become active.</p> <p>See the <a href="#">“Configuring the Outgoing Proxy Bypass List”</a> section on page 5-42.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Outgoing Proxy</b>                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Outgoing Proxy Hostname                       | Hostname or IP address of the outgoing proxy. The first host name or IP address entered designates that outgoing proxy server as the primary server. You can configure up to eight proxy servers. If the primary fails to respond, the request is redirected to the next proxy server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Outgoing Proxy Port                           | Enter the port number the proxy server uses to receive requests.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Acquirer Outgoing Proxy Authentication</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Username                                      | If authentication is required, enter a username. This username is used for both NTLM and basic authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Password                                      | Enter the password for the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Table 5-17 HTTP Connections Fields (continued)**

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Confirm Password                   | Re-enter the password for the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| NTLM User Domain                   | The NTLM server domain name used to authenticate the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Disable Basic Authentication       | If checked, basic authentication will not occur as a fallback to an NTLM authentication failure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Outgoing HTTP Proxy Bypass Domains | <p>If an incoming HTTP request matches a domain configured in this list, it will not be forwarded to the configured HTTP proxy server. The request will be routed according to its destination FQDN.</p> <p>This field is activated when you select the Enable Outgoing Proxy check box. Separate up to 32 outgoing proxy domain entries with a space. See <a href="#">Figure 5-15</a>.</p> <p>See also the “Configuring the Outgoing Proxy Bypass List” section on <a href="#">page 5-42</a>.</p>                                                                                |
| Outgoing HTTP Proxy Bypass List    | <p>If an incoming HTTP request matches the IP address or subnet configured in this list, it will not be forwarded to the configured HTTP proxy server. The request will be routed according to its destination IP address.</p> <p>This field is activated when you select the Enable Outgoing Proxy check box. Separate up to 32 outgoing proxy bypass addresses with a space (entered in CIDR notation, for example 10.10.10.10/24). See <a href="#">Figure 5-15</a>.</p> <p>See also the “Configuring the Outgoing Proxy Bypass List” section on <a href="#">page 5-42</a>.</p> |

**Figure 5-14 HTTP Connections Settings Page**

The screenshot displays the 'HTTP Connection Settings' page for Service Engine **cc-sre910-1**. The interface includes a left-hand navigation menu with options like 'Device Home', 'Device Activation', 'Assignments', 'Replication', 'Request Routing', 'Service Control', 'Application Control', 'Default and Maximum Bandwidth', 'Bandwidth Schedules', 'Windows Media Streaming', 'Movie Streamer', 'RTSP Advanced Settings', 'Flash Media Streaming', 'Web', and 'HTTP'. The 'HTTP' section is expanded, showing 'HTTP Connections', 'HTTP Caching', 'HTTP Cache Freshness', 'Advanced HTTP Caching', and 'HTTPS'.

The main content area shows the following settings:

- Webengine Maximum Concurrent Connections:** 2000 (range 100-12000)
- Enable IP Spoofing:** ☒
- Enable Incoming Proxy:** ☒ Space separated list of incoming HTTP ports: 80
- Enable Outgoing Proxy:** ☒

The **Outgoing Proxy** section contains a table with the following columns: Hostname, Port, Username, Password, Confirm Password, NTLM User Domain, and Disable basic authentication.

|     | Hostname       | Port | Username | Password | Confirm Password | NTLM User Domain | Disable basic authentication |
|-----|----------------|------|----------|----------|------------------|------------------|------------------------------|
| 1 * | 128.107.241.17 | 80   |          |          |                  |                  | <input type="checkbox"/>     |
| 2   |                |      |          |          |                  |                  | <input type="checkbox"/>     |

## Configuring the Outgoing Proxy Bypass List

The bypass function allows a service engine to skip the forwarding of some HTTP requests to the proxy bypass server based on destination domain or IP address.

To configure the Outgoing Proxy Bypass list:

- Step 1** Choose **Devices > Devices > Application Control > Web > HTTP > HTTP Connections**.
- Step 2** Select the **Enable Outgoing Proxy** check box. The Outgoing Proxy fields become active (Figure 5-15).
- Step 3** Enter either domains or IP addresses to be bypassed by the outgoing proxy in the Outgoing Proxy Bypass Domains textbox or Outgoing Proxy Bypass List textbox, respectively. Each entry is separated by a single space.
  - a. List of domains: Domain entries can be either a fully qualified domain name or a general domain. For example, a FQDN entry of `ecds.cisco.com` will bypass proxying of all requests intended for that server. An entry of `cisco.com` will bypass all sub-domains within `cisco.com`, including `ecds.cisco.com`.
  - b. List of subnets/IP addresses: Subnets and IP addresses should be entered in CIDR notation. For example, the subnet `10.10.10.0` should be entered in the form `10.10.10.0/24`. Single IP addresses must be in CIDR notation, with 32 as the CIDR subnet suffix. For example, the IP address `10.10.10.10` should be entered in the form `10.10.10.10/32`.
- Step 4** To configure outgoing proxy bypass lists using CLI, proceed to [Outgoing Proxy Bypass Commands](#).

**Figure 5-15** Enabling Outgoing HTTP Proxy Bypass

HTTP Connection Settings for Service Engine, gluon

HTTP Connection Settings will be enabled when using Factory Defaults. The values shown in this page are in effect.

**HTTP Connection Settings**

Current settings: None (Using Factory Defaults)

Webengine Maximum Concurrent Connections: \* 2000 (100-12000)

Enable IP Spoofing: ☐

Enable Incoming Proxy: ☐ Space separated list of incoming HTTP ports: \* 80

Enable Outgoing Proxy: ☒

| Outgoing Proxy |          |      |          | Acquirer Outgoing Proxy Authentication |                  |                  |                              |
|----------------|----------|------|----------|----------------------------------------|------------------|------------------|------------------------------|
|                | Hostname | Port | Username | Password                               | Confirm Password | NTLM User Domain | Disable basic authentication |
| 1 *            |          |      |          |                                        |                  |                  | <input type="checkbox"/>     |
| 2              |          |      |          |                                        |                  |                  | <input type="checkbox"/>     |
| 3              |          |      |          |                                        |                  |                  | <input type="checkbox"/>     |
| 4              |          |      |          |                                        |                  |                  | <input type="checkbox"/>     |
| 5              |          |      |          |                                        |                  |                  | <input type="checkbox"/>     |
| 6              |          |      |          |                                        |                  |                  | <input type="checkbox"/>     |
| 7              |          |      |          |                                        |                  |                  | <input type="checkbox"/>     |
| 8              |          |      |          |                                        |                  |                  | <input type="checkbox"/>     |

Outgoing HTTP Proxy Bypass Domains: cisco.com california.com Space separated list of up to 32 Domains

Outgoing HTTP Proxy Bypass List: 11.1.1.0/24 12.2.3.4/32 Space separated list of up to 32 Addresses (entered in CIDR notation i.e. 10.10.10.10/24)

- Step 5** Click **Submit** to save the settings.
  - To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

### Outgoing Proxy Bypass Commands

**Step 1** To add a domain to the outgoing proxy bypass list, enter the following command:

```
SE(config)# http proxy outgoing bypass domain-name [domain]
```

Multiple domains can be added to the outgoing proxy bypass list using the follow format:

```
SE(config)# http proxy outgoing bypass domain-name [domain 1] [domain 2] ...
```

Up to 32 domains can be entered.

**Step 2** To remove a domain from the outgoing proxy bypass list, enter the following command:

```
SE(config)# no http wmt proxy outgoing bypass domain-name [domain 1] [domain 2]...
```

Multiple domains can be removed at a time.

**Step 3** To add a single IP address to the outgoing proxy bypass list, enter the following command:

```
SE(config)# http proxy outgoing bypass ip-address [IP-address] subnet-mask 255.255.255.255
```

**Step 4** To add a subnet to the outgoing proxy bypass list, enter the following command:

```
SE(config)# http proxy outgoing bypass ip-address [IP-address] subnet-mask [Netmask]
```



**Note** The mask address is not in CIDR notation, but is in standard IP mask notation, for example 255.255.255.0.

**Step 5** To remove an IP address or subnet from the outgoing proxy bypass list, enter the following command:

```
SE(config)# no http proxy outgoing bypass ip-address [IP-address] subnet-mask [Netmask]
```

## Configuring Web Engine HTTP Caching

To configure web engine HTTP caching:

**Step 1** Choose **Devices > Devices > Application Control > Web > HTTP > HTTP Caching**. The HTTP Caching page is displayed ([Figure 5-16](#)).

Figure 5-16 HTTP Caching Page

The screenshot shows the Cisco Enterprise Content Delivery System Manager interface. The top navigation bar includes 'Devices', 'Services', and 'System'. The left sidebar shows a tree view with 'Application Control' expanded, and 'HTTP Caching' selected under 'Web'. The main content area is titled 'HTTP Caching for Service Engine, cc-sre910-1'. It contains a section for 'HTTP Caching' with the following settings:

| HTTP Caching                                    |                          |
|-------------------------------------------------|--------------------------|
| Current settings: None (Using Factory Defaults) |                          |
| Min Object Size.*                               | 0 (Bytes) (0-4294967295) |
| Max Object Size.*                               | 0 (MB) (0-2047)          |

Note: \* - Required Field

At the bottom right, there are 'Submit' and 'Cancel' buttons.

- Step 2** In the Min Object Size field, enter the minimum content object size that the SE will cache. The range is from 0 to 4294967295 bytes.
- Step 3** In the Max Object Size field, enter the maximum content object size that the SE will cache. The range is from 0 to 2047 megabytes. Zero (0) means no limit.
- Step 4** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring Web Engine HTTP Cache Freshness

To configure the web engine HTTP cache freshness:

- Step 1** Choose **Devices > Devices > Application Control > Web > HTTP > HTTP Cache Freshness**. The HTTP Cache Freshness page is displayed (Figure 5-17).

**Figure 5-17 HTTP Cache Freshness Page**

The screenshot shows the 'HTTP Cache Freshness Settings' page for Service Engine, NE-612-5. The left-hand navigation pane includes sections like 'Device Home', 'Device Activation', 'Assignments', 'Replication', 'Service Control', 'Application Control', 'Default and Maximum Bandwidth', 'Bandwidth Schedules', 'Windows Media Streaming', 'Movie Streamer', 'RTSP Advanced Settings', 'Web', 'HTTP', 'HTTP Connections', 'HTTP Caching', 'HTTP Cache Freshness', 'Advanced HTTP Caching', 'General Settings', and 'Monitoring'. The 'HTTP Cache Freshness' option is selected. The main content area shows the following settings:

- Enable:** A checkbox that is currently unchecked.
- Object Age Multiplier:** A text input field containing the value '30'.
- Max TTL Scale:** A dropdown menu currently set to 'days'.
- Max Object TTL:** A text input field containing the value '1'.
- Minimum TTL:** A text input field containing the value '30', with '(Minutes)' indicated to the right.
- Enable Re-evaluate Request All:** A checkbox that is currently unchecked.

A note at the bottom states: 'Note: \* - Required Field'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

- Step 2** Enter the settings as appropriate. Table 5-18 describes the fields.

**Table 5-18 HTTP Cache Freshness Fields**

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable                | When checked, HTTP cache freshness is enabled.                                                                                                                                                                                                                                                                                                                                |
| Object Age Multiplier | The age multiplier value (as a percentage) enables the SE to guess the life of an object by multiplying the time since the object was last modified by a percentage to obtain an approximate expiration date. After this date, the object is considered stale, and subsequent results cause a fresh retrieval by the SE. The range is from 0 to 100. The default value is 30. |
| Max TTL Scale         | The scale (seconds, hours, minutes, or days) to use for the Max Object TTL. The time-to-live (TTL) sets a ceiling on estimated expiration dates. If an object has an explicit expiration date, this takes precedence over the configured TTL. The default is days.                                                                                                            |

**Table 5-18 HTTP Cache Freshness Fields (continued)**

| Field                          | Description                                                                                                                                                                                            |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Object TTL                 | The maximum time-to-live (TTL) for objects in cache. The ranges are as follows:<br>1 to 1825 days<br>1 to 43800 hours<br>1 to 2628000 minutes<br>1 to 157680000 seconds<br><br>The default is 61 days. |
| Minimum TTL                    | The minimum time-to-live (in minutes) for objects in the cache. The range is from 0 to 86400. The default value is 60.                                                                                 |
| Enable Re-evaluate Request All | When enabled, all requests are re-evaluated, whether for objects or directory listings.                                                                                                                |

**Step 3** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring Web Engine Advanced HTTP Caching

To configure web engine advanced HTTP cache settings:

**Step 1** Choose **Devices > Devices > Application Control > Web > HTTP > Advanced HTTP Caching**. The Advanced HTTP Caching page is displayed ([Figure 5-18](#)).

**Figure 5-18 Advanced HTTP Caching Page**

Advanced HTTP Caching for Service Engine, farnsworth

Advanced HTTP Caching will be enabled when using Factory Defaults. The values shown in this page are in effect.

**Advanced HTTP Caching**

Current settings: None (Using Factory Defaults)

Enable Cache Cookies: ☐

Enable Cache NonCacheable: ☐

Enable Cache Query String: ☐

Enable Cache Fill Range: ☐

Enable Cache On Abort: ☐

Abort Percent Threshold:  (0-99)

Note: \* - Required Field

**Step 2** Enter settings as appropriate using the information in [Table 5-19](#) as a guide.



**Table 5-19**      **Advanced HTTP Caching Fields**

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Cache Cookies       | When enabled, the Web engine caches requests with a cookie header in the response.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Enable Cache NonCacheable  | When enabled, caches web objects that are not supposed to be cached. By default the box is not checked.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Enable Cache Query String  | <p>Provides the option to cache query strings in the Web Engine cache. A query string is the part of a URL that contains data that is passed to web applications. A typical URL containing a query string:</p> <p>http://server/path/program?query_string.</p> <p><b>Tip</b>      The question mark is used as a separator and is not part of the query string.</p> <p>Requests with query string parameters are cached separately for each unique query string only if an expiration time is specified; if the HTTP header field does not have an expiration header, it will not be cached. Each request is stored as a separate file in the WE.</p> |
| Enable Cache Fill Range    | When enabled, the complete content is cached when the range request for the same is given by the client. The range request starts with zero (0).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Enable Cache on Abort      | <p>When enabled, caching an object is continued even though the client has aborted the request.</p> <p><b>Note</b>      The <b>Abort Percentage Threshold</b> field must be set for content to be cached when the client aborts.</p>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Use Percentage Threshold   | When enabled, caches an object if the percentage of the object already downloaded is greater than the percentage threshold value entered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Abort Percentage Threshold | <p>The percentage threshold at which the content is still cached even if the client aborts.</p> <p><b>Note</b>      To ensure content is cached when the client aborts, set the Abort Percentage Threshold to a very small value.</p>                                                                                                                                                                                                                                                                                                                                                                                                                 |

**Step 3**      Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

# Configuring HTTPS

**Note**

HTTPS works only in WCCP transparent proxy mode when WCCP is enabled; if WCCP is not enabled, the HTTPS server cannot be enabled.

**Prerequisites**

To configure HTTPS for WCCP, you must do the following:

1. Configure WCCP. See the [“Configuring WCCP General Settings” section on page 7-1](#) to enable WCCP.
2. Import a self-signed certificate from a selected webserver to enable HTTPS cache.

**Note**

The steps for importing self-signed certificates and keys are beyond the scope of the Cisco ECDS Configuration Guide. There are various types of HTTPS servers and each has its own procedures for generating self-signed certificates and keys. Refer to your HTTPS server for instructions.

3. Create HTTPS service in the Enterprise Content Delivery System Manager GUI or by using the **https server** global configuration command. To verify that HTTPS is enabled successfully on your system, use the **show https server** command.
4. Assign the certificate and associate a key with the HTTPS server.

**Note**

Once you have completed these prerequisites, the Service Engine performs a certificate-hostname to HTTPS-Server-hostname comparison, and an HTTPS certificate import validation before HTTPS can be enabled on your system. HTTPS cannot be enabled on the Service Engine unless these conditions are met.

**Restrictions**

Observe these restrictions for certificates, keys, and certificate groups after they have been created and are in use:

- A certificate without valid imported values cannot be associated with a certificate group.
- A certificate group without added certificates cannot be associated with an HTTPS server.
- A certificate used by an HTTPS server cannot be modified or deleted.
- A certificate group used by an HTTPS server cannot be modified or deleted.
- A certificate added to a certificate group cannot be modified or deleted.
- A key used by an HTTPS server cannot be modified or deleted.

**Tip**

Certificates, keys, and certificate groups can be modified or deleted when they are not in use.

**Procedure**

Configure, modify, and view HTTPS settings for Service Engines and device groups:

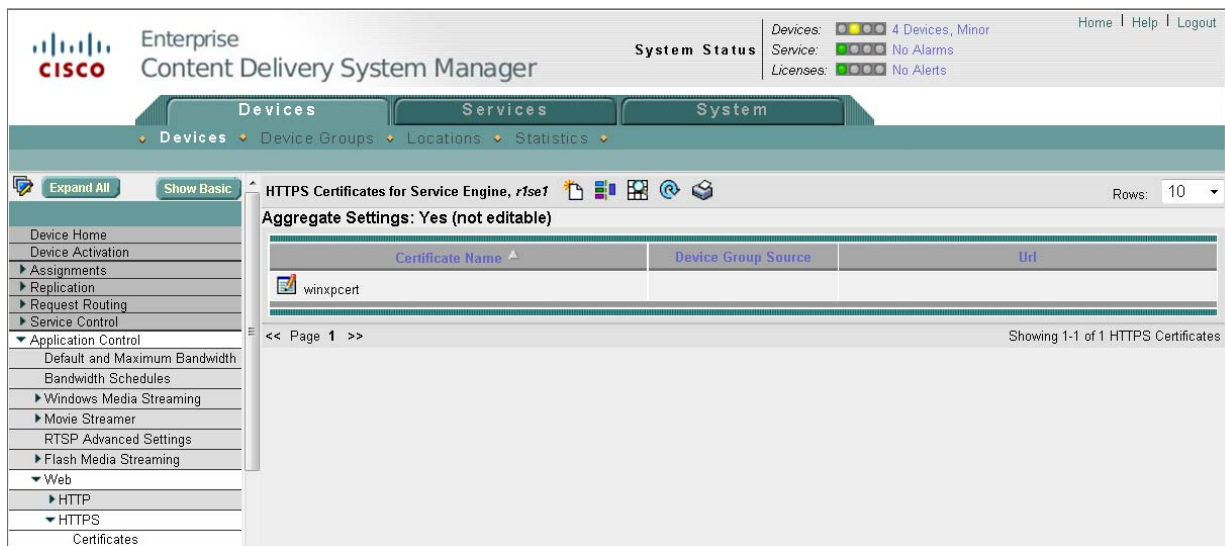
- [Configuring HTTPS Certificates, page 5-49](#)
- [Configuring HTTPS Certificate Groups, page 5-54](#)
- [Configuring HTTPS Keys, page 5-57](#)
- [Configuring HTTPS Servers, page 5-60](#)
- [HTTPS Configuration Examples, page 5-63](#)

**Configuring HTTPS Certificates**

To configure HTTPS certificates for the Service Engine after you have imported the necessary certificates and keys:

- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the ECDS network.
- Step 2** Click the **Edit** icon next to the Service Engine for which you want to configure HTTPS certificates. The Device Home for Service Engine window appears.
- Step 3** In the Contents pane, choose **Application Control > Web > HTTPS > Certificates**. The HTTPS Certificates for Service Engine window appears. The certificates created for device groups can only be viewed; they cannot be modified ([Figure 5-19](#)).

**Figure 5-19** *HTTPS Certificates*



Use the **https cert EXEC** command to create certificate objects with a given name, to import a certificate from external sources into a certificate object, or to remove existing certificate objects.

- Step 4** To create a new HTTPS digital certificate, click the **Create New HTTPS Certificate** icon in the taskbar. The HTTPS Certificate window appears ([Figure 5-20](#)). [Table 5-20](#) describes the fields.

Figure 5-20 HTTPS Certificate for Service Engine

Table 5-20 HTTPS Certificate Settings

| GUI Parameter    | Function                                                                                                                     | CLI Command                                                       |
|------------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Certificate Name | (Required) Name of the certificate.<br><b>Tip</b> Key/Cert must be imported using HTTP or FTP protocol.                      | <b>https cert <i>cert_name</i> create</b>                         |
| Certificate URL  | External location from which the certificate is to be imported.<br><b>Tip</b> The URL must be a valid URL using HTTP or FTP. | <b>https cert <i>cert_name</i> import url <i>FTP/HTTP URL</i></b> |
| Username         | Username required to access the external source from which the certificate is being imported.                                | —                                                                 |
| Password         | Password used to authenticate users who want to gain access to the external source.                                          | —                                                                 |
| Confirm Password | Verifies the password entry.                                                                                                 | —                                                                 |

**Step 5** In the Certificate Name field, specify the name of the certificate. Certificate names must consist solely of alphanumeric, underscore, and hyphen characters. Certificate names can begin with a numeric character. Certificate names can have a maximum length of 64 characters.

**Tip**

You need to create a certificate before importing its value from an external source associating it with an HTTPS server. Only certificate names are stored in the CMS database; the actual certificates are stored on the Service Engine.

Once you have created a certificate, you cannot modify the name. You need to delete the existing certificate and create a new one.

- Step 6** In the Certificate URL field, specify the external location from which the certificate is to be imported. The URL must be a valid URL using HTTP or FTP. The certificate value is imported after you specify the URL and submit changes.

A certificate name without imported values can be listed in the ECDS Manager GUI; however, only certificates with valid values can be associated with an HTTPS server or added to a certificate group. Two different certificates can be imported from the URL and two different HTTPS servers can be associated with the same certificate.



**Tip** After a certificate is imported from the ECDS GUI, a new icon (**Re-import**) appears in the taskbar. The **Re-import** icon can be used to reimport the certificates if the import operation did not succeed the first time. For information about the task bar icons, see the [“Configuring Bandwidth for Replication and Ingest” section on page 5-6](#).

- Step 7** In the Username field, specify the username required to access the external source from which the certificate is being imported. An entry is required in this field only if the external source is password-protected.
- Step 8** In the Password field, specify the password used to authenticate users who want to gain access to the external source from which the certificate is being imported. An entry is required in this field only if the external source is password-protected. Reenter the password in the Confirm Password field.
- Step 9** Click **Submit** to save the settings.



**Tip** To edit an HTTPS certificate, click the **Edit** icon next to the HTTPS certificate that you want to edit.

## Filtering HTTPS Certificates for the Service Engine

Use the ECDS GUI to filter and display a subset of HTTPS certificates by certificate name and URL. To set the filter criteria to display selected HTTPS certificates:

- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the ECDS network.
- Step 2** Click the **Edit** icon next to the Service Engine for which you want to filter HTTPS certificate groups. The Device Home for Service Engine window appears with the Contents pane on the left.
- Step 3** In the Contents pane, choose **Application Control > Web > HTTPS > Certificate Groups**. The HTTPS Certificates for Service Engine window appears. The certificates created for device groups can only be viewed; they cannot be modified.
- Step 4** Click the **Filter Table** icon in the taskbar. The Filtering HTTPS Certificates for Service Engine window appears ([Figure 5-21](#)).

**Figure 5-21 Filtering HTTPS Certificates for Service Engine**

The screenshot shows the Cisco Enterprise Content Delivery System Manager interface. The top navigation bar includes 'Devices', 'Services', and 'System'. The 'System Status' section shows: Devices: 1 Device, Critical; Service: 3 Services, Minor; Licenses: No Alerts. The left sidebar contains a tree view with 'Application Control' expanded, showing 'Default and Maximum Bandwidth', 'Bandwidth Schedules', 'Windows Media Streaming', 'Movie Streamer', 'RTSP Advanced Settings', 'Flash Media Streaming', 'Web', 'HTTP', and 'HTTPS'. The 'HTTPS' section is selected, showing 'Certificates', 'Certificate Groups', 'Keys', and 'Servers'. The main content area is titled 'Filtering HTTPS Certificates for Service Engine, fai-mde1100'. It contains two filter criteria: 'Certificate Name: like' and 'Certificate URL: like'. Below these are instructions for the LIKE and NOT LIKE operators, and for the IN and NOT IN operators. At the bottom right are 'Submit' and 'Cancel' buttons.

Enterprise Content Delivery System Manager

System Status

Devices: 1 Device, Critical  
Service: 3 Services, Minor  
Licenses: No Alerts

Home | Help | Logout

Devices | Services | System

Devices | Device Groups | Locations | Statistics

Expand All | Show Basic

Device Home  
Device Activation  
Assignments  
Replication  
Request Routing  
Service Control  
Application Control  
Default and Maximum Bandwidth  
Bandwidth Schedules  
Windows Media Streaming  
Movie Streamer  
RTSP Advanced Settings  
Flash Media Streaming  
Web  
HTTP  
HTTPS  
Certificates  
Certificate Groups  
Keys  
Servers

Filtering HTTPS Certificates for Service Engine, fai-mde1100

Certificate Name: like

Certificate URL: like

Note for the LIKE and NOT LIKE operators:

- % - Matches any string of zero or more characters except null
- Matches any single character
- ESCAPE character
- Any character, excepting percent (%) and underscore (\_) may follow the ESCAPE character
- A wildcard character will be treated as a literal if preceded by the ESCAPE character

Note for the IN and NOT IN operators:

- Accepts a list of comma separated strings. eg: itemA, itemB, itemC
- Accepts valid sql syntax. eg: ('itemA', 'itemB', 'itemC')
- Use single quotes (') when a comma and/or parentheses are part of the item's name. eg: itemA, 'item,B', '(itemC)'

Submit Cancel

- Step 5** Choose a filter operator from the Certificate Name drop-down list and enter the name of the certificate that must be matched. [Table 5-21](#) describes the filter operators for filtering HTTPS certificates.
- Step 6** Choose a filter operator from the Certificate URL drop-down list and enter the certificate location that must be matched.
- Step 7** Click **Submit**. The HTTPS Certificates for Service Engine window reappears, displaying a list of all certificates that match the specified filter criteria.

**Table 5-21 Filtering HTTPS Certificates**

| Filter Operators | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Like             | <p>Include HTTPS certificates with a setting that is similar to the string entered. Use the percent sign (%) wildcard characters to match zero or more characters, and use the underscore (_) wildcard character to match exactly one character. If the string contains special characters such as ^, (, ), or ', use the escape character, a backslash (\), to ignore the meaning of such special characters. Any character except a % or _ can follow the escape character. Wildcard characters following an escape character are treated as literal characters.</p> <p>For example, to display HTTPS certificates with names that begin with <b>httpscer</b> and are followed by a single character, enter <b>httpscer_</b> in the Certificate Group Name field. Any certificate with the name Httpscer is not displayed.</p> |
| Not like         | <p>Includes HTTPS certificates with a setting that is not similar to the string entered. Use the percent sign (%) wildcard characters to match zero or more characters, and use the underscore (_) wildcard character to match exactly one character. If the string contains special characters such as ^, (, ), or ', use the escape character, a backslash (\), to ignore the meaning of such special characters. Any character except a % or _ can follow the escape character. Wildcard characters following an escape character are treated as literal characters.</p> <p>For example, to display HTTPS certificates except the ones with URLs that start with ftp://, enter %ftp:// in the Certificate URL field. Any certificate with the URL https://a.com or http://a.com is displayed.</p>                             |
| In               | <p>Includes certificates with settings that are present in the list of specified strings. You can specify either a single string or a list of strings separated by commas. Use single quotes (') when the specified string contains commas or parentheses.</p> <p>For example, to display certificates with names CER1, CER2, and CER(3), enter (CER1,CER2,'CER(3)') or CER1,CER2,'CER(3)' in the Certificate Name field. Certificates with names such as CER4 and CER5 are not displayed.</p>                                                                                                                                                                                                                                                                                                                                   |
| Not in           | <p>Includes certificates with settings that are not present in the list of specified strings. You can specify either a single string or a list of strings separated by commas. Use single quotes (') when the specified string contains commas or parentheses.</p> <p>For example, to display certificates except the ones with names CER1, CER2, and CER(3), enter (CER1,CER2,'CER(3)') or CER1,CER2,'CER(3)' in the Certificate Name field. Certificates with names such as CER4 and CER5 are displayed</p>                                                                                                                                                                                                                                                                                                                    |

**Table 5-21 Filtering HTTPS Certificates (continued)**

| Filter Operators | Description                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Equal to         | Includes certificates with a setting that is exactly the same as the string entered.<br><br>For example, to display all certificates imported from the URL <code>http://Location1</code> , enter <code>http://Location1</code> in the Certificate URL field. Certificates imported from <code>http://Location^1</code> are not displayed. You cannot use keywords, special characters, or wildcard characters.     |
| Not equal to     | Includes certificates with a setting that is not exactly the same as the string entered.<br><br>For example, to display all certificates not imported from the URL <code>http://Location1</code> , enter <code>http://Location1</code> in the Certificate URL field. Certificates imported from <code>http://Location^1</code> are displayed. You cannot use keywords, special characters, or wildcard characters. |

## Configuring HTTPS Certificate Groups

Certificate groups represent a trust relationship chain from root Certificate Authority to end entity. Each certificate in a certificate group (except the end entity's certificate) signs and trusts the next one in the chain. An end entity's certificate can be trusted only if all certificates in the certificate group leading to this certificate can be trusted. A certificate group can be used to represent an HTTPS server just like a single certificate, but with the added benefit that the client does not need to have all certificates locally. A certificate group can also be used to verify and authenticate an HTTPS server by comparing the server's certificates to the those of the certificate group.



### Note

Certificates must be added to a certificate group in the following order:

1. Identity certificate
2. Intermediate certificate
3. Root certificate

To configure HTTPS certificate groups for the Service Engine:

- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the ECDS network.
- Step 2** Click the **Edit** icon next to the Service Engine for which you want to filter HTTPS certificate groups. The Device Home for Service Engine window appears with the Contents pane on the left.
- Step 3** In the Contents pane, choose **Application Control > Web > HTTPS > Certificate Groups**. The HTTPS Certificate Groups for Service Engine window appears. The certificate groups created for device groups can only be viewed; they cannot be modified.

The **https certgroup EXEC** command allows you to create or remove certificate groups or import a certificate from an external source and add it to an existing certificate chain.



- Step 4** To create a new HTTPS digital certificate group, click the **Create New HTTPS Certificate Group** icon in the taskbar. The HTTPS Certificate Group for Service Engine window appears. You can create certificate groups with a given name, and add specified existing certificates to the current certificate group using this window (Figure 5-22). Table 5-22 describes the fields.

**Figure 5-22** HTTPS Certificate Group

**Table 5-22** HTTPS Certificate Group Settings

| GUI Parameter          | Function                                                                                                                                                                                          | CLI Command                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Certificate Group Name | Name of the certificate group.                                                                                                                                                                    | <b>https certgroup</b><br><i>certgroup_name create</i>                                                        |
| Certificate 1, 2, 3... | Certificate chain to use for the HTTPS server.<br><br><b>Tip</b> Add certificates to the certificate chain starting with the identity cert, the intermediate cert, and finally to root CA's cert. | <b>https certgroup</b><br><i>certgroup_name add-cert</i><br><i>cert_name1 cert_name2</i><br><i>cert_name3</i> |

- Step 5** In the Certificate Group Name field, specify the name of the certificate group to be used for certificate chains and server certificate authentication. Certificate group names must consist solely of alphanumeric, underscore, and hyphen characters. Certificate group names can begin with a numeric character. Certificate group names can have a maximum of 64 characters.



**Note** Once you have created a certificate group name, you cannot change it. You need to delete the existing certificate group and create a new one.

- Step 6** Choose the name of the certificate to be added to the certificate group from the Certificate drop-down lists. All certificates created using the HTTPS Certificates for Service Engine window are listed here. You can add a maximum of six certificates per certificate group.

- Step 7** Two different certificate groups can have the same combination of HTTPS certificates. You can choose up to six certificates from the Certificate drop-down lists 1 through 6. These drop-down lists are set to an initial value of **Do not set**. You must choose these certificates in sequence when you add them to the certificate group and each associated certificate must be unique, or an error message is displayed when you click **Submit**.
- Step 8** To delete a certificate group, click the **Delete HTTPS Certificate Group** icon in the taskbar. You cannot delete a certificate group that is referenced by an HTTPS server. You must remove the association between the certificate group and HTTPS server before deleting.
- Step 9** To view a subset of the entire list of HTTPS certificate groups, click the **Filter Table** icon in the taskbar. See the next section “[Filtering HTTPS Certificate Groups for the Service Engine](#),” for more details.
- Step 10** To revert to the display of all configured HTTPS certificate groups, click the **View All HTTPS Certificate Groups** icon in the taskbar.
- Step 11** Click **Submit** to save the settings.



**Tip** To edit an HTTPS certificate group, click the **Edit** icon next to the HTTPS certificate group that you want to edit.

## Filtering HTTPS Certificate Groups for the Service Engine

Use the ECDS Manager GUI to filter and display a subset of HTTPS certificate groups by certificate group name.

To set the filter criteria to display selected HTTPS certificate groups:

- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the ECDS network.
- Step 2** Click the **Edit** icon next to the Service Engine for which you want to filter HTTPS certificate groups. The Device Home for Service Engine window appears with the Contents pane on the left.
- Step 3** In the Contents pane, choose **Application Control > Web > HTTPS > Certificate Groups**. The HTTPS Certificate Groups for Service Engine window appears. The certificate groups created for device groups can only be viewed; they cannot be modified.
- Step 4** Click the **Filter Table** icon in the taskbar. The Filtering HTTPS Certificate Groups for Service Engine window appears.
- Step 5** Choose a filter operator from the Certificate Group Name drop-down list, and enter the name of the certificate group that must be matched.
- Step 6** To revert to the display of all configured HTTPS certificate groups, click the **View All HTTPS Certificate Groups** icon in the taskbar. [Table 5-21](#) describes example filter operators for filtering HTTPS certificate groups.
- Step 7** Click **Submit**. The HTTPS Certificate Groups for Service Engine window reappears, displaying a list of all certificate groups that match the specified filter criteria.

## Configuring HTTPS Keys

The private key is the secret half of a key pair used in a public key algorithm. Private keys are typically used to encrypt a symmetric session key, digitally sign a message, or decrypt a message that has been encrypted with the corresponding public key. PKCS #12 specifies a portable format for storing or transporting a user's private keys and certificate information. The private key that the Service Engine uses to act as an origin HTTPS server must match the selected certificate.

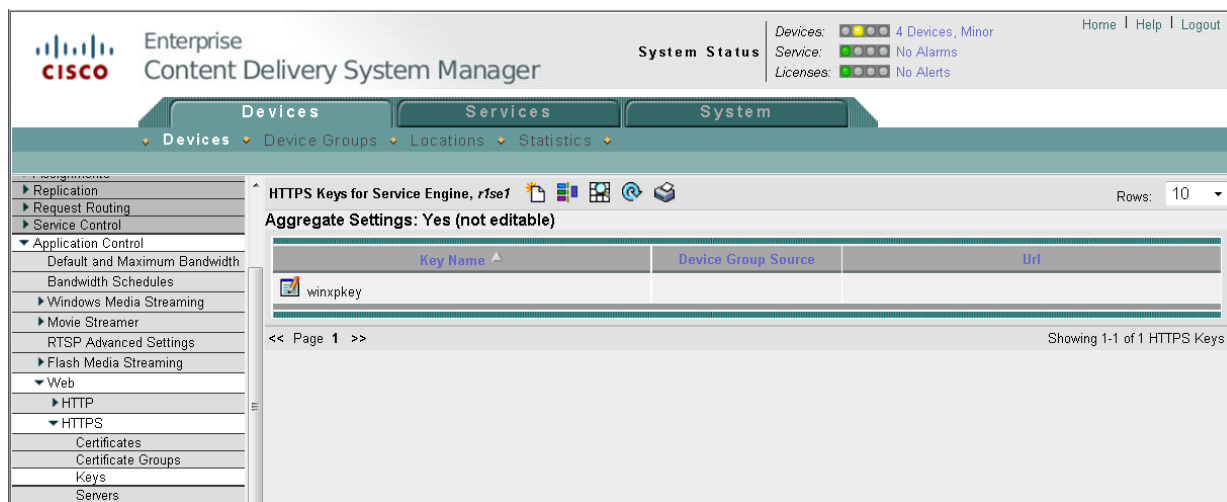
You can create keys with a given name, import keys from external sources, or remove existing keys using the CDSM.

To configure HTTPS keys for the Service Engine:

- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the ECDS network.
- Step 2** Click the **Edit** icon next to the Service Engine for which you want to configure HTTPS keys. The Device Home for Service Engine window appears.
- Step 3** In the **Contents** pane, choose **Application Control > Web > HTTPS > Keys**. The HTTPS Keys for Service Engine window appears. The keys created for device groups can only be viewed; they cannot be modified (Figure 5-23).

Use the **https key EXEC** command to create a private key object with a given name, to import a private key object from an external source, or to remove a private key object with a given name.

**Figure 5-23** HTTPS Keys



- Step 4** To create a new HTTPS key, click the **Create New HTTPS Key** icon in the taskbar to configure an HTTPS key. The Creating new HTTPS Key for Service Engine window appears (Figure 5-24). Table 5-23 describes the fields.

Figure 5-24 HTTPS Certificate Key

The screenshot displays the 'HTTPS Key for Service Engine, fa1-mde1100' configuration page in the Cisco Enterprise Content Delivery System Manager. The page features a left-hand navigation pane with various system management options. The main content area contains a form with the following fields: 'Key Name' (marked as required), 'Key URL', 'Username', 'Password', and 'Confirm Password'. A 'Note' at the bottom indicates that fields marked with an asterisk are required. At the bottom right of the form are 'Submit' and 'Cancel' buttons. The top of the interface shows the 'System Status' and a summary of system components: 1 Device (Critical), 3 Services (Minor), and No Alerts.

Table 5-23 HTTPS Key Settings

| GUI Parameter | Function                                                                                                                            | CLI Command                                                        |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Key Name      | Name of the key.<br><b>Tip</b> Key/Cert must be imported using HTTP or FTP protocol                                                 | <b>https key</b> <i>key_name</i>                                   |
| Key URL       | External location from which the private key is to be imported.<br><b>Tip</b> The URL must be a valid URL using HTTP, FTP, or HTTPS | <b>https key</b> <i>key_name</i> <b>import</b> <i>FTP/HTTP URL</i> |

- Step 5** In the **Key Name** field, specify the name of the private key to be imported from an internal or external certificate authority (CA). You need to create a private key before importing its value from an external source and associating it with an HTTPS server. Key names must consist solely of alphanumeric, underscore, and hyphen characters. Key names can begin with a numeric character. Key names can have a maximum length of 64 characters.



**Note** Once you have created the name of an HTTPS key, you cannot modify it. You need to delete the existing key and create a new one. Only HTTPS key names are stored in the ECDS database. The actual certificates are stored on the Service Engine.

- Step 6** In the **Key URL** field, specify the external location from which the private key is to be imported. The URL must be a valid URL using HTTP, FTP, or HTTPS. The key value is imported when you specify the URL and submit changes.

A key name without imported values can be listed in the ECDS Manager GUI; however, only keys with valid values can be associated with an HTTPS server. Two different keys can be imported from the URL and two different HTTPS servers can be associated with the same key.

After a key is imported from the ECDS Manager GUI, a new icon (**Re-import**) appears in the taskbar. The **Re-import** icon can be used to reimport the key if the import did not succeed the first time.

- Step 7** In the **Username** field, specify the username required to access the external source from which the key is being imported. An entry is required in this field only if the external source is password-protected.
- Step 8** In the **Password** field, specify the password used to authenticate users who want to gain access to the external source from which the key is being imported. An entry is required in this field only if the external source is password-protected. Reenter the password in the **Confirm Password** field.



**Note** Use only non-encrypted keys when setting up the HTTPS server; only non-encrypted keys are supported. See the [“Configuring HTTPS Servers”](#) section on page 5-60.

- Step 9** To view a subset of the entire list of HTTPS keys, click the **Filter Table** icon in the taskbar. See the next section [“Filtering HTTPS Keys for the Service Engine”](#) for more details.
- Step 10** To revert to the display of all configured HTTPS keys, click the **View All HTTPS Keys** icon in the taskbar.
- Step 11** Click **Submit** to save the changes.



**Tip** To edit an HTTPS key, click the **Edit** icon next to the HTTPS key that you want to edit.

## Filtering HTTPS Keys for the Service Engine

Use the ECDS Manager GUI to filter and display a subset of HTTPS keys by the private key name and URL.

To set the filter criteria to display selected HTTPS keys:

- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the ECDS network.
- Step 2** Click the **Edit** icon next to the Service Engine for which you want to filter HTTPS keys. The Device Home for Service Engine window appears with the Contents pane on the left.
- Step 3** In the Contents pane, choose **Application Control > Web > HTTPS > Keys**. The HTTPS Keys for Service Engine window appears. The keys created for device groups can only be viewed; they cannot be modified.
- Step 4** Click the **Filter Table** icon in the taskbar. The Filtering HTTPS Keys for Service Engine window appears.
- Step 5** Choose a filter operator from the **Key Name** drop-down list and enter the name of the key that must be matched.
- Step 6** Choose a filter operator from the **Key URL** drop-down list and enter the key location that must be matched.
- Step 7** To revert to the display of all configured HTTPS keys, click the **View All HTTPS Keys** icon in the taskbar. [Table 5-21](#) describes example filter operators for filtering HTTPS keys.

- Step 8** Click **Submit**. The HTTPS Keys for Service Engine window reappears, displaying a list of all keys that match the specified filter criteria.

## Configuring HTTPS Servers

You can configure an HTTPS server and configure a caching solution to allow a Service Engine act as an origin HTTPS server. This configuration reduces WAN traffic and increases data security because authorized clients from remote branch offices can access their own Service Engines, which are configured as HTTPS servers, by using HTTPS.

The Service Engine decodes HTTPS traffic from a client and performs normal HTTP operations on it, such as caching and request processing. The Service Engine will initiate HTTPS connections to an origin server and fetch content from origin servers upon a cache miss or cache validation.



### Note

When setting up the HTTPS server, choose only non-encrypted keys from the available keys drop-down menu. Only non-encrypted keys are supported.

To configure HTTPS servers for the Service Engine:

- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the ECDS network.
- Step 2** Click the **Edit** icon next to the Service Engine for which you want to configure HTTPS servers. The Device Home for Service Engine window appears.
- Step 3** In the Contents pane, choose **Application Control > Web > HTTPS > Servers**. The HTTPS Servers for Service Engine window appears (Figure 5-25).

**Figure 5-25** HTTPS Servers for Service Engine

The screenshot shows the Cisco Enterprise Content Delivery System Manager interface. The top navigation bar includes 'Devices', 'Services', and 'System'. The left sidebar shows a tree view with 'Application Control' expanded, and 'Web' > 'HTTPS' > 'Servers' selected. The main content area displays the 'HTTPS Servers for Service Engine, r1se1' configuration page. It includes a table with columns: Server Name, Device Group Source, Enable, Port, Certificate, Server Certificate Group, Authenticating Certificate Group, and Private Key. Two servers are listed: 'winxp' and 'winxp2'. The 'winxp' server has 'Enable' set to 'false' and 'Port' 443. The 'winxp2' server has 'Enable' set to 'true' and 'Port' 488. Both servers use 'winxpcert' as the Certificate and 'winxpkey' as the Private Key. The 'Server Certificate Group' and 'Authenticating Certificate Group' are both set to 'None'. The page also shows 'Aggregate Settings' with 'Yes' selected, and a status bar at the bottom indicating 'Showing 1-2 of 2 HTTPS Servers'.

| Server Name | Device Group Source | Enable | Port | Certificate | Server Certificate Group | Authenticating Certificate Group | Private Key |
|-------------|---------------------|--------|------|-------------|--------------------------|----------------------------------|-------------|
| winxp       |                     | false  | 443  | winxpcert   | None                     | None                             | winxpkey    |
| winxp2      |                     | true   | 488  | winxpcert   | None                     | None                             | winxpkey    |

Use the **https server** command to manage the HTTPS server on the Service Engine.

- Step 4** The Aggregate Settings **Yes** radio button is selected by default. This means that HTTPS servers are displayed for the Service Engine as well as for any associated device groups. The settings for the HTTPS servers for device groups cannot be modified or deleted; they are read-only. However, you can modify the HTTPS servers for the Service Engine. If you click the **Aggregate Settings No** radio button, you can view and modify the HTTPS servers for the Service Engine only. The HTTPS servers for any associated device groups are not even displayed.
- Step 5** To create a new HTTPS server, click the **Create New HTTPS Server** icon in the taskbar. The Creating new HTTPS Server for Service Engine window appears.

Configure settings in the following sections of the window:

- HTTPS Servers (Figure 5-26)
- Certificate Key/Associations (Figure 5-27)

**Figure 5-26** Creating New HTTPS Server for Service Engine - HTTPS Servers

- Step 6** In the **HTTPS Server** section, follow these steps:
- In the **Name** field, specify the name of the HTTPS server. Server names can consist of Arabic numerals and upper- and lowercase alphabetic, underscore, hyphen, and period characters. Server names must begin with an alphabetic character or underscore and have a limit of 15 characters.
  - To enable caching and SSL termination for the HTTPS server, check the **Enable** check box. You must have entered the host name, certificate or certificate group, and private key before an HTTPS server can be enabled.
  - In the **Host Name** field, specify the IP address or fully qualified domain name for the origin HTTPS server. Two different HTTPS servers cannot have the same host name.  
  
Each active server has one or more IP addresses associated with it, specified either as an IP address or a domain name that is resolved to one or more IP addresses. An HTTPS request arriving at a Service Engine (either by WCCP intercept or by direct proxy) is matched with a server configuration that will be used to handle the request by comparing the target IP address of the request with the IP addresses associated with the active servers.
  - In the **Port** field, specify the port number that will accept redirected HTTPS traffic.

**Figure 5-27** Creating New HTTPS Server for Service Engine - Certificate Key/Association



**Step 7** In the **Certificate Key/Associations** section, follow these steps:

- a. Choose the certificate group for the HTTPS server from the **Server Certificate** drop-down list. All certificate groups created using the HTTPS Certificate Groups for Service Engine window will be displayed here.

The certificate group is included in the SSL handshake that is sent to SSL clients. Only one certificate group can be selected for an HTTPS server at a time.



**Note** SSL Version 2 does not support certificate groups.

- b. From the **Certificate** drop-down list, choose a specific SSL certificate so that the Service Engine can act as an origin HTTPS server while authenticating clients. All certificates created using the HTTPS Certificates for Service Engine window are displayed here. Only one certificate can be selected for an HTTPS server at a time ([Figure 5-28](#)).

**Figure 5-28** Configuring Certificate and Key

- c. From the **Private Key** drop-down list, choose a non-encrypted private key so that the Service Engine can act as an origin HTTPS server while authenticating clients. This private key must match the selected certificate. All keys created using the HTTPS Keys for Service Engine window are displayed here. See [Configuring HTTPS Keys](#) for more information.



**Note** Only one key can be selected for an HTTPS server at a time and the key that you choose must be non-encrypted.

**Step 8** Leave the **Private Key Password** field empty.



**Note** Only non-encrypted keys are supported.

**Step 9** Select the Identity certificate for the origin server before submitting the request to create a new HTTPS server

**Step 10** Click **Submit** to save the settings.



**Tip** To edit an HTTPS server, click the **Edit** icon next to the HTTPS server that you want to edit.



## Filtering HTTPS Servers for the Service Engine

Use the ECDS Manager GUI to filter and display a subset of HTTPS servers by server name, status (enabled or disabled), host name, SSL cache size, SSL cache timeout, protocol version, status of server certificate authentication (enabled or disabled), and status of server certificate authentication error tracking (enabled or disabled).

To set the filter criteria to display selected HTTPS servers:

- 
- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the ECDS network.
  - Step 2** Click the **Edit** icon next to the Service Engine for which you want to filter HTTPS servers. The Device Home for Service Engine window appears with the Contents pane on the left.
  - Step 3** In the Contents pane, choose **Application Control > Web > HTTPS > HTTPS Servers**. The HTTPS Servers for Service Engine window appears.
  - Step 4** Click the **Filter Table** icon in the taskbar. The Filtering HTTPS Server Entries for Service Engine window appears.
  - Step 5** From the **Name** drop-down list, choose a filter operator, and enter the name of the server that must be matched.
  - Step 6** From the **Enable** drop-down list, choose a filter operator, and from the second drop-down list, choose whether or not you want to view servers on which HTTPS caching is enabled.
  - Step 7** From the **Host** drop-down list, choose a filter operator, and enter the IP address or fully qualified domain name of the host that must be matched.
  - Step 8** Click **Submit**. The HTTPS Servers for Service Engine window reappears, displaying a list of all servers that match the specified filter criteria. [Table 5-21](#) describes example filter operators for filtering HTTPS servers for the Service Engine.
  - Step 9** To revert to the display of all configured HTTPS servers, click the **View All HTTPS Servers** icon in the taskbar.
- 

## HTTPS Configuration Examples

The following example shows how to load the certificates and private key on the Service Engine:

```
ServiceEngine# https cert mycert create
ServiceEngine# https cert mycert import http://www.myca.com/myservercert
ServiceEngine# https cert mykey create
ServiceEngine# https cert mykey import http://www.myca.com/myprivatekey
```

The following example shows that when you enter the **https server test** command from the global configuration prompt, the CLI prompt changes:

```
ServiceEngine(config)# https server test
ServiceEngine(config-https)#
```

The following example shows that you can then enter the specific commands required to configure the HTTPS server without having to repeatedly type the **https server name** command:

```
ServiceEngine(config-https)# cert testcert
ServiceEngine(config-https)# key testkey
ServiceEngine(config-https)# host www.mycompany-testserver.com
ServiceEngine(config-https)# port 443
ServiceEngine(config-https)# enable
```

Use the **show statistics https requests** EXEC command to determine how many HTTPS requests go through the Service Engine.

Use the **show bypass list** EXEC command to determine whether the origin HTTPS server has been added to the WCCP accept list.

The following example displays the output from the **show running-configuration** EXEC command entered on a Service Engine with the HTTPS server enabled:

```
ServiceEngine# show running-config
!
!
wccp router-list 1 10.77.157.217
wccp https-cache router-list-num 1 password ****
wccp version 2
!
https server UNI certgroup chain uni-group
https server UNI key uni-key password ****
https server UNI host 10.77.157.170
https server UNI enable
https server DSA210 certgroup chain dsa-group
https server DSA210 key dsa-210-key password ****
https server DSA210 host 10.77.157.210
https server DSA210 enable
https server test-w2k cert iis-crt
https server test-w2k key iis-key password ****
https server test-w2k host 10.77.140.131
https server test-w2k enable
```

### HTTPS Debugging

HTTPS debugging is combined with debugging the web engine. Enter the **debug webengine trace** command to enable HTTPS debugging.



**Tip**

Remember that enabling HTTPS debugging can slow down the performance of HTTP(S) significantly.

### HTTPS Statistics

HTTPS statistics information can be found using **http statistics** command. There is no special statistics command available for HTTPS.

## General Settings

The General Settings pages provide settings for access control of the device, maintenance, network connectivity, and monitoring:

- [Configuring Content Management, page 5-65](#)
- [Login Access Control, page 5-65](#)
- [Authentication, page 5-71](#)
- [Scheduling Database Maintenance, page 5-75](#)
- [Setting Storage Handling, page 5-76](#)
- [Network Settings, page 5-77](#)
- [Configuring Notification and Tracking, page 5-95](#)

- [Enabling the Kernel Debugger for Troubleshooting, page 5-109](#)
- [Configuring Service Router Settings, page 5-109](#)

## Configuring Content Management

To configure the maximum number of entries for cache content:

- 
- |               |                                                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Devices &gt; Devices</b> . The Devices Table page is displayed.                                                                                                                                                                                                                                        |
| <b>Step 2</b> | Click the <b>Edit</b> icon next to the device you want to configure. The Devices home page is displayed.                                                                                                                                                                                                         |
| <b>Step 3</b> | Click <b>Show All</b> to display the top-level menu options.                                                                                                                                                                                                                                                     |
| <b>Step 4</b> | Choose <b>General Settings &gt; Content Management</b> . The Content Management page is displayed.                                                                                                                                                                                                               |
| <b>Step 5</b> | In the <b>Max Cache Content Entries</b> field, enter the value for the maximum entries of cached content allowed. The range is from 1 to 10,000,000. The default is 3,000,000.                                                                                                                                   |
| <b>Step 6</b> | Click <b>Submit</b> to save the settings. <ul style="list-style-type: none"><li>• To apply the factory default settings for the device, click the <b>Apply Defaults</b> icon in the task bar.</li><li>• To remove the settings from the device, click the <b>Remove Settings</b> icon in the task bar.</li></ul> |
- 

## Login Access Control

Login authentication and authorization are used to control user access and configuration rights to CDSMs, SEs, and SRs. Login authentication is the process by which the devices verify whether the person who is attempting to log in to the device has a valid username and password. The person logging in must have a user account registered with the device. User account information serves to authorize the user for login and configuration privileges. The user account information is stored in an authentication, authorization, and accounting (AAA) database, and the devices must be configured to access the particular authentication server (or servers) where the AAA database is kept.

In an ECDS network, user accounts can be created for access to the CDSM and, independently, for access to the SEs and SRs that are registered to the CDSM. For user accounts that access the CDSM, see the [“Configuring AAA” section on page 9-1](#).

See the following sections for more information:

- [Login Authentication, page 5-66](#)
- [Configuring SSH, page 5-68](#)
- [Enabling Telnet, page 5-68](#)
- [Setting the Message of the Day, page 5-69](#)
- [Changing the CLI Session Time, page 5-70](#)
- [Changing Users—Admin Password, page 5-70](#)
- [Creating, Editing, and Deleting Users—Usernames, page 5-70](#)
- [Viewing Network Interfaces, page 5-82](#)

## Login Authentication

Login authentication provides the configuration for independent logins (login access to the device only).

Login authentication can also be used to log in to the CDSM GUI. When logging in to the CDSM GUI with an external user account (RADIUS or TACACS+), the user is authenticated by the external database. After the external user is authenticated, its role depends on the privilege configured in the external database (zero [0] means a normal user and 15 means a super user). The privilege level of 0 or 15 is mapped to the read-only or admin user role in the CDSM GUI. No CDSM local user is created in the CDSM database for the external user that logs in, so the external user cannot be managed by the CDSM GUI.

**Note**

If you plan to use a RADIUS server or a TACACS+ server for authentication, you must configure the RADIUS or TACACS+ server settings before you configure and submit the login authentication settings in the [Procedure](#) below. See the [“Configuring RADIUS Server Settings” section on page 5-72](#) and the [“Configuring TACACS+ Server Settings” section on page 5-73](#) to set up these servers.

When the primary login server and the primary configuration server are set to local, usernames and passwords are local to each device. Local authentication and authorization uses locally configured login and passwords to authenticate login attempts.

By default, local login authentication is enabled. You can disable local login authentication only after enabling one or more of the other login authentication servers. However, when local login authentication is disabled, if you disable all other login authentication methods, a warning message is displayed stating “At least one authentication method is required to select for login.”

**Note**

Authentication login and authentication configuration are required for the local user to login.

**Caution**

Make sure that RADIUS or TACACS+ authentication is configured and operating correctly before disabling local authentication and authorization. If you disable local authentication and RADIUS or TACACS+ is not configured correctly, or if the RADIUS or TACACS+ server is not online, you may be unable to log in to the device.

**Procedure**

To configure the login authentication and configuration authorization schemes for the device:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Login Access Control > Login Authentication**. The Login Authentication page is displayed.
- Step 5** Enter the settings as appropriate. See [Table 5-24](#) for a description of the fields.

**Table 5-24 Login Authentication Fields**

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Failover Server Unreachable | If Enable Failover Server Unreachable is enabled, the device fails over to the secondary server only if the primary server is unreachable. In any other case, for example, the authentication fails in the RADIUS server, the local database is not contacted for authentication. Conversely, if the Enable Failover Server Unreachable option is disabled, the device contacts the secondary server, regardless of the reason the authentication failed with the primary server. |
| Authentication Login Servers       | Required for local user login. When enabled, authentication login servers are used to authenticate user logins.                                                                                                                                                                                                                                                                                                                                                                   |
| Primary Login Server               | Choose local, RADIUS, or TACACS+.<br>Command example:<br><code>SE(config)# authentication login radius enable primary</code>                                                                                                                                                                                                                                                                                                                                                      |
| Secondary Login Server             | Choose local, RADIUS, or TACACS+.<br>Command example:<br><code>SE(config)# authentication login tacacs enable secondary</code>                                                                                                                                                                                                                                                                                                                                                    |
| Tertiary Login Server              | Choose local, RADIUS, or TACACS+.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Authentication Config Server       | Required for local user login. When enabled, authentication configuration servers are used to authenticate user privileges.                                                                                                                                                                                                                                                                                                                                                       |
| Primary Config Server              | Choose local, RADIUS, or TACACS+.<br>Command example:<br><code>SE(config)# authentication configuration tacacs enable primary</code>                                                                                                                                                                                                                                                                                                                                              |
| Secondary Config Server            | Choose local, RADIUS, or TACACS+.<br>Command example:<br><code>SE(config)# authentication configuration local enable secondary</code>                                                                                                                                                                                                                                                                                                                                             |
| Tertiary Config Server             | Choose local, RADIUS, or TACACS+.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**Step 6** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

**Note**

User is allowed to execute the configuration command based on privilege levels specified in TACACS+server after being authenticated by TACACS+server

**Note**

The commands like "authentication login" and "authentication configuration" are not mutually exclusive and both are required for each authentication method.

## Configuring SSH

Secure Shell (SSH) consists of a server and a client program. Like Telnet, you can use the client program to remotely log in to a machine that is running the SSH server. However, unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication.

The SSH page allows you to specify the key length and login grace time.

To enable the SSH daemon:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Login Access Control > SSH**. The SSH page is displayed.
  - Step 5** Check **Enable** to enable the SSH feature. SSH enables login access to the device through a secure and encrypted channel.
  - Step 6** In the **Length of Key** field, specify the number of bits needed to create an SSH key. The default is 2048.
  - Step 7** In the **Login Grace Time** field, specify the number of seconds the server waits for the user to successfully log in before it ends the connection. The authentication procedure must be completed within this time limit. The default is 300 seconds.



---

**Note** When changing the **Login Grace Time**, you need to first uncheck the **Enable** check box and click **Submit**. Enter the new **Login Grace Time**, check **Enable**, and click **Submit**.

---

- Step 8** Select the SSH version:
  - a. To allow clients to connect using SSH protocol version 1, check the **Enable SSHv1** check box.
  - b. To allow clients to connect using SSH protocol version 2, check the **Enable SSHv2** check box.



---

**Note** You can enable both SSHv1 and SSHv2, or you can enable one version and not the other. You cannot disable both versions of SSH unless you disable the SSH feature by unchecking the **Enable** check box.

---

- Step 9** Click **Submit** to save the settings.
    - To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
    - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Enabling Telnet

To enable the Telnet service:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.

- Step 4** Choose **General Settings > Login Access Control > Telnet**. The Telnet page is displayed.
- Step 5** Check **Telnet Enable** to enable the terminal emulation protocol for remote terminal connections.
- Step 6** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Setting the Message of the Day

The Message of the Day (MOTD) feature enables you to provide information bits to the users when they log in to a device. There are three types of messages that you can set up:

- MOTD banner
- EXEC process creation banner
- Login banner

To configure the Message of the Day settings:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Login Access Control > Message of the Day**. The MOTD page is displayed.
- Step 5** Check **Enable** to enable the MOTD settings. The Message of the Day (MOTD) banner, EXEC process creation banner, and Login banner fields become enabled.
- Step 6** In the **Message of the Day (MOTD) Banner** field, enter a string that you want to display as the MOTD banner when a user attempts to log in to the device.



**Note** In the Message of the Day (MOTD) Banner, EXEC Process Creation Banner, and Login Banner fields, you can enter a maximum of 980 characters. A new line character (or **Enter**) is counted as two characters, as it is interpreted as \n by the system. You cannot use special characters such as ` , % , ^ , and " in the MOTD text.

---

- Step 7** In the **EXEC Process Creation Banner** field, enter a string to be displayed as the EXEC process creation banner when a user enters into the EXEC shell of the device.
- Step 8** In the **Login Banner** field, enter a string to be displayed after the MOTD banner when a user attempts to log in to the device.
- Step 9** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
-

## Changing the CLI Session Time

To change the CLI session time:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Login Access Control > CLI Session Time**. The CLI Session Time page is displayed.
  - Step 5** In the **CLI Session Time** field, enter the time (in minutes) that the device waits for a response before ending the session.
  - Step 6** Click **Submit** to save the settings.
    - To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
    - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Changing Users—Admin Password

Every device (CDSM, SE, and SR) has a built-in user account. The username is *admin* and the default password is *default*. This account allows access to all services and entities in the ECDS. Any user that can access the Admin Password page in the CDSM can configure a new password for the administrator user account on individual SEs and SRs.

To change the Admin password:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Login Access Control > Users > Admin Password**. The Admin Password page is displayed.
  - Step 5** In the **Password** field, enter a new password.
  - Step 6** In the **Confirm Password** field, re-enter the password.
  - Step 7** Click **Submit** to save the settings.
    - To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
    - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Creating, Editing, and Deleting Users—Usernames

You can create, edit, and delete user accounts for login access to individual devices or device groups. A privilege profile must be assigned to each new user account. The Usernames page uses privilege profiles to determine which tasks a user can perform and the level of access provided. Users with administrative privileges can add, delete, or modify user accounts through the CDSM or the device CLI.



To create, edit, or delete a user account:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Login Access Control > Users > Usernames**. The User Table page is displayed.
- The table is sortable by clicking the column headings.
- For information about Aggregate Settings, see the [“Managing Aggregate Settings” section on page 4-8](#)
- Step 5** Click the **Create New** icon in the task bar. The Local User page is displayed.
- To edit a local user, click the **Edit** icon next to the name you want to edit.
- Step 6** Enter the settings as appropriate. See [Table 5-25](#) for a description of the fields.

**Table 5-25 Local User Fields**

| Field            | Description                                                                                                                                                                                                                                                                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username         | Name of user.                                                                                                                                                                                                                                                                                                            |
| Password         | User password.                                                                                                                                                                                                                                                                                                           |
| Confirm Password | Re-enter user password.                                                                                                                                                                                                                                                                                                  |
| Privilege        | There are two types of predefined privilege profiles: <ul style="list-style-type: none"><li>• Normal user—User has read access and can see some of the SE, SR, or CDSM settings.</li><li>• Superuser—User has administrative privileges such as creating new users and modifying the SE, SR, or CDSM settings.</li></ul> |

- Step 7** Click **Submit** to save the settings.
- To delete a user, click the **Edit** icon for the user, then click the **Delete** icon in the task bar.
- 

## Authentication

User authentication and authorization (configuration rights) data can be maintained in any combination of these three databases:

- Local database (located on the device)
- RADIUS server (external database)
- TACACS+ server (external database)

The Login Authentication page allows you to choose an external access server or the internal (local) device-based authentication, authorization, and accounting (AAA) system for user access management. You can choose one method or a combination of the three methods. The default is to use the local database for authentication.

See the following sections for more information:

- [Configuring RADIUS Server Settings, page 5-72](#)
- [Configuring TACACS+ Server Settings, page 5-73](#)
- [Configuring an Access Control List \(ACL\), page 5-74](#)

## Configuring RADIUS Server Settings

To use RADIUS for login or configuration authentication, choose **General Settings > Login Access Control > Login Authentication**. See the [“Login Authentication” section on page 5-66](#).



### Note

The CDSM does not cache user authentication information. Therefore, the user is reauthenticated against the Remote Authentication Dial In User Service (RADIUS) server for every request. To prevent performance degradation caused by many authentication requests, install the CDSM in the same location as the RADIUS server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

To configure the RADIUS server settings:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Authentication > RADIUS Server**. The RADIUS Server Settings page is displayed.
- Step 5** Enter the settings as appropriate. See [Table 5-26](#) for a description of the fields.

**Table 5-26 RADIUS Server Settings Fields**

| Field                  | Description                                                                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable RADIUS Servers  | Enables RADIUS authentication.                                                                                                                                        |
| Time to wait           | Number of seconds to wait for a response before timing out on a connection to a RADIUS server. The range is from 1 to 20. The default is 5.<br>Use the tacacs timeout |
| Number of retransmits  | Number of attempts allowed to connect to a RADIUS server. The default is 2.                                                                                           |
| Enable redirect        | Redirects an authentication response to a different authentication server if an authentication request using the RADIUS server fails.                                 |
| Redirect Message [1-3] | Message sent to the user if redirection occurs.<br><b>Note</b> If the redirect message has a space, it must be in quotes (“ ”).                                       |
| Location [1-3]         | Sets an HTML page location. This is the URL destination of the redirect message that is sent when authentication fails.                                               |
| Shared Encryption Key  | Encryption key shared with the RADIUS server. The maximum number of characters allowed is 15.                                                                         |
| Server Name [1-5]      | IP address or hostname of the RADIUS server.                                                                                                                          |
| Server Port [1-5]      | Port number on which the RADIUS server is listening. The default is 1645.                                                                                             |

**Step 6** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring TACACS+ Server Settings

To use TACACS+ for login or configuration authentication, choose **General Settings > Login Access Control > Login Authentication**. See the “[Login Authentication](#)” section on page 5-66.



### Note

The CDSM does not cache user authentication information. Therefore, the user is reauthenticated against the Terminal Access Controller Access Control System Plus (TACACS+) server for every request. To prevent performance degradation caused by many authentication requests, install the CDSM in the same location as the TACACS+ server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.



### Tip

TACACS+ users log into the ECDS and their privilege level is maintained on the TACACS server and not on the Cisco ECDS locally. TACACS+ users with privilege level 15 (super user) can execute any command without the enable password. TACACS+ users with privilege level 0 are placed in enable mode and must type the enable password to get into configuration mode.

To configure the TACACS+ server settings:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Authentication > TACACS+ Server**. The TACACS+ Server Settings page is displayed.
- Step 5** Enter the settings as appropriate. See [Table 5-27](#) for a description of the fields.

**Table 5-27 TACACS+ Server Settings Fields**

| Field                             | Description                                                                                               |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------|
| Enable TACACS+ Servers            | Enables TACACS+ authentication.                                                                           |
| Use ASCII Password Authentication | Changes the default password type from Password Authentication Protocol (PAP) to ASCII clear text format. |

**Table 5-27 TACACS+ Server Settings Fields (continued)**

| Field                               | Description                                                                                                                                  |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Time to wait                        | Number of seconds to wait for a response before timing out on a connection to a TACACS+ server. The range is from 1 to 20. The default is 5. |
| Number of retransmits               | Number of attempts allowed to connect to a TACACS+ server. The default is 2.                                                                 |
| Security Word                       | Encryption key shared with the TACACS+ server.                                                                                               |
| Primary Server                      | IP address or hostname of the primary TACACS+ server.                                                                                        |
| Secondary Server<br>Tertiary Server | IP address or hostname of the backup TACACS+ server. Up to two backup servers are allowed.                                                   |

**Step 6** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring an Access Control List (ACL)



### Note

If your system is configured for WCCP, skip this section; ACLs are not supported with WCCP.

To configure an access control list (ACL) for group authorization:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Authentication > Access Control List > Configure Access Control List**. The Access Control List Table page is displayed.  
The table is sortable by clicking the column headings.
- Step 5** Click the **Create New** icon in the task bar. The Configure Access Control List page is displayed.  
To edit a group, click the **Edit** icon next to the name you want to edit.
- Step 6** Enter the settings as appropriate. See [Table 5-28](#) for a description of the fields.

**Table 5-28 Access Control List Fields**

| Field  | Description                                      |
|--------|--------------------------------------------------|
| Action | Whether to permit or deny access for this group. |

**Table 5-28 Access Control List Fields (continued)**

| Field           | Description                                                                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Name      | If this action is for all groups, choose <b>Any Group Name</b> .<br>If this action is for a specific group, choose <b>Enter Group Name</b> and enter the group name in the field. |
| Change Position | To change the order of this group in the access control list, which is displayed in the Access Control List Table page, click <b>Change Position</b> .                            |

**Step 7** Click **Submit** to save the settings.

To delete a group, click the **Edit** icon for the group, then click the **Delete** icon in the task bar.

**Step 8** From the left-panel menu, choose **Enable Access Control List**. The Enable Access Control List page is displayed.

**Step 9** Check the **Enable Access Control List** check box and click **Submit**.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- To move a group up or down in the Access Control List table, click the Up arrow or Down arrow in the Move column.

The ACL can be applied from the device or from a device group. The source of the currently applied settings is shown in the Access Control List Table page.

## Scheduling Database Maintenance

The database maintenance runs at the scheduled time only when the following three conditions are satisfied:

- Last vacuum process happened more than 30 minutes in the past.
- Percent increase in disk space usage is greater than 10 percent.
- Available free disk space is greater than 10 percent of the total disk space.

If any of these conditions are not satisfied, the database maintenance does not run at the scheduled time.

To schedule a database cleaning or reindexing:

**Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.

**Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.

**Step 3** Click **Show All** to display the top-level menu options.

**Step 4** Choose **General Settings > Database Maintenance**. The Database Maintenance Settings page is displayed.

**Step 5** Enter the settings as appropriate. See [Table 5-29](#) for a description of the fields.

**Table 5-29 Database Maintenance Settings Fields**

| Field                                        | Description                                                                                                 |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Full Database Maintenance Settings</b>    |                                                                                                             |
| Enable                                       | When enabled, a full database maintenance routine is performed on the device.                               |
| Every Day                                    | The days of the week when the maintenance is performed                                                      |
| Sun-Sat                                      | When Every Day is enabled, all days of the week are also enabled.                                           |
| At (time)                                    | Time of day the maintenance is performed. Time is entered in 24-hour format as hh:mm. The default is 04:00. |
| <b>Regular Database Maintenance Settings</b> |                                                                                                             |
| Enable                                       | When enabled, a re-indexing routine is performed on the device.                                             |
| Every Day                                    | The days of the week when the maintenance is performed.                                                     |
| Sun-Sat                                      | When Every Day is enabled, all days of the week are also enabled.                                           |
| At (time)                                    | Time of day the maintenance is performed. Time is entered in 24-hour format as hh:mm. The default is 02:00. |

**Step 6** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Setting Storage Handling

The Disk Error Handling page allows you to configure how disk errors are handled, and to define a disk device error-handling threshold.

If a bad disk drive is a critical disk drive, and the automatic reload feature (**disk error-handling reload** command) is enabled, the disk drive is marked as “bad” and the device is automatically reloaded. After the device is reloaded, a syslog message and an SNMP trap are generated.

The disk error-handling threshold option determines how many disk errors can be detected before the disk drive is automatically marked “bad.” By default, this threshold is set to 10.

For information about repairing latent sector errors (LSEs) on a disk, see the [“Disk Latent Sector Error Handling” section on page 11-19](#).

To configure a disk error-handling method:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Storage > Disk Error Handling**. The Disk Error Handling Settings page is displayed.
- Step 5** Check the **Enable** check box.

- Step 6** Check the **Enable Disk Error Handling Reload** check box if you want the device to reload the disk when a disk with a system file system (sysfs) has problems.
- Step 7** Check the **Enable Disk Error Handling Threshold** check box if you want to set the number of disk errors allowed before the disk is marked as bad, and enter a number (0 to 100) in the **Threshold** field. The default threshold is 10.
- Step 8** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Network Settings

The Network pages provide settings for network connectivity. Go to **Devices > General Settings > Network** to configure the following procedures:

- [Enabling FTP Services, page 5-77](#)
- [Enabling DNS, page 5-78](#)
- [Enabling RCP, page 5-78](#)
- [Configuring NTP, page 5-79](#)
- [Setting the Time Zone, page 5-79](#)
- [Viewing Network Interfaces, page 5-82](#)
- [Configuring External IP Addresses, page 5-82](#)
- [Configuring Port Channel and Load Balancing Settings, page 5-83](#)
- [Configuring IP General Settings, page 5-83](#)
- [Configuring IP ACL, page 5-84](#)
- [Configuring Static IP Routes, page 5-94](#)
- [Configuring DSR VIP, page 5-95](#)

## Enabling FTP Services

To enable FTP services to listen for connection requests:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Network > FTP**. The FTP Settings page is displayed.
- Step 5** Check the **Enable FTP Services** check box.
- Step 6** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
-

## Enabling DNS

DNS Settings are required on all SEs, SRs, and CDSMs. The SEs need to be able to resolve the content origin server host name, the SRs need to be able to communicate with the DNS servers, and the CDSMs need to resolve host names.

To configure Domain Name System (DNS) servers:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Network > DNS**. The DNS Settings page is displayed.
  - Step 5** Enter the settings as appropriate. See [Table 5-30](#) for a description of the fields.

**Table 5-30 DNS Settings Fields**

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable              | Enables Domain Name System (DNS) on the device.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| List of DNS Servers | Space-delimited list of IP addresses for up to eight name servers for name and address resolution.                                                                                                                                                                                                                                                                                                                                                                            |
| Domain Names        | A space-delimited list of up to three default domain names. A default domain name allows the system to resolve any unqualified hostnames. Any IP hostname that does not contain a domain name will have the configured domain name appended to it. This appended name is resolved by the DNS server and then added to the host table. A DNS server must be configured on the system for hostname resolution to work correctly. To do this, use the List of DNS Servers field. |

- Step 6** Click **Submit** to save the settings.
    - To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
    - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Enabling RCP

Remote Copy Protocol (RCP) lets you download, upload, and copy configuration files between remote hosts and a switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection oriented. This service listens for requests on TCP port 514.

To enable RCP services:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Network > RCP**. The RCP page is displayed.



- Step 5** Check the **RCP Enable** check box to have the RCP services listen for RCP requests.
- Step 6** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring NTP

To configure the device to synchronize its clock with an NTP server:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Network > NTP**. The NTP page is displayed.
- Step 5** Check **Enable** to enable NTP.
- Step 6** In the **NTP Server** field, enter the IP address or hostname of up to four NTP servers. Use a space to separate the entries.
- Step 7** Enter the **ntp server <ntp-server-IP>** command to ensure that the Service Engine will work properly with Flash Media Streamer and to successfully sync with CDSM.
- Step 8** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Setting the Time Zone

If you have an outside source on your network that provides time services, such as an NTP server, you do not need to set the system clock manually. When manually setting the clock, enter the local time. The device calculates Coordinated Universal Time (UTC) based on the time zone set.



### Note

Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at startup to initialize the software clock.



### Caution

We highly recommend that you use NTP servers to synchronize the devices in your ECDS network. If you change the local time on the device, you must change the BIOS clock time as well; otherwise, the timestamps on the error logs are not synchronized. Changing the BIOS clock is required because the kernel does not handle time zones.

To manually configure the time zone:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.

- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Network > Time Zone**. The Time Zone page is displayed with the default settings of UTC (offset = 0) and no daylight savings time configured.
- Step 5** To configure a standard time zone:

- a. Click the **Standard Time Zone** radio button.

The standard convention for time zones uses a *Location/Area* format in which *Location* is a continent or a geographic region of the world and *Area* is a time zone region within that location. For a list of standard time zones that can be configured and their UTC offsets, see [Table 5-31 on page 5-81](#).

- b. From the **Standard Time Zone** drop-down list, choose a location for the time zone. The page refreshes, displaying all area time zones for the chosen location in the second drop-down list.
- c. Choose an area for the time zone.

The UTC offset (hours and minutes ahead or behind UTC) for the corresponding time zone is displayed. During summer time savings, the offset may differ and is displayed accordingly.



**Note** Some of the standard time zones (mostly time zones within the United States) have daylight savings time zones configured automatically.

- Step 6** To configure a customized time zone:
- a. Click the **Customized Time Zone** radio button.
- b. In the **Customized Time Zone** field, enter a name for the time zone. The time zone entry is case sensitive and can contain up to 40 characters. Spaces are not allowed. If you specify any of the standard time zone names, an error message is displayed when you click **Submit**.
- c. For UTC offset, choose + or – from the **UTC Offset** drop-down list to indicate whether the configured time zone is ahead or behind UTC. Also, choose the number of hours (0 to 23) and minutes (0 to 59) offset from UTC for the customized time zone. The range for the UTC offset is from –23:59 to 23:59, and the default is 0:0.

- Step 7** To configure customized summer time savings:



**Note** Customized summer time can be specified for both standard and customized time zones.

The start and end dates for summer time can be configured in two ways: absolute dates or recurring dates. Absolute dates apply once and must be reset every year. Recurring dates apply every year.

- a. Click the **Absolute Dates** radio button to configure summer settings once.
- b. In the **Start Date** and **End Date** fields, specify the month, day, and year that the summer time savings starts and ends in mm/dd/yyyy format.
- Alternatively, click the **Calendar** icon and select a date. The chosen date is highlighted in blue. Click **Apply**.
- c. Click the **Recurring Dates** radio button to configure a recurring summer setting.
- d. Using the drop-down lists, choose the start day, week, and month when the summer time savings starts. For example, if the summer time savings begins the first Sunday in March, you would select Sunday, 1st, March from the drop-down lists.

- e. Using the drop-down lists, choose the start day, week, and month when the summer time savings ends.
- Step 8** Using the **Start Time** drop-down lists and the **End Time** drop-down lists, choose the hour (0 to 23) and minute (0 to 59) at which daylight savings time starts and ends.
- Start Time and End Time fields for summer time are the times of the day when the clock is changed to reflect summer time. By default, both start and end times are set at 00:00.
- Step 9** In the Offset field, specify the minutes offset from UTC (0 to 1439). (See [Table 5-31 on page 5-81](#).)
- The summer time offset specifies the number of minutes that the system clock moves forward at the specified start time and backward at the end time.
- Step 10** To not specify a summer or daylight savings time for the corresponding time zone, click the **No Customized Summer Time Configured** radio button.
- Step 11** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.

[Table 5-31](#) lists the UTC offsets for the different locations around the world.

**Table 5-31 Time Zone—Offset from UTC**

| Time Zone            | Offset from UTC (in hours) | Time Zone           | Offset from UTC (in hours) |
|----------------------|----------------------------|---------------------|----------------------------|
| Africa/Algiers       | +1                         | Asia/Vladivostok    | +10                        |
| Africa/Cairo         | +2                         | Asia/Yekaterinburg  | +5                         |
| Africa/Casablanca    | 0                          | Asia/Yakutsk        | +9                         |
| Africa/Harare        | +2                         | Australia/Adelaide  | +9.30                      |
| Africa/Johannesburg  | +2                         | Australia/Brisbane  | +10                        |
| Africa/Nairobi       | +3                         | Australia/Darwin    | +9.30                      |
| America/Buenos_Aires | −3                         | Australia/Hobart    | +10                        |
| America/Caracas      | −4                         | Australia/Perth     | +8                         |
| America/Mexico_City  | −6                         | Australia/Sydney    | +10                        |
| America/Lima         | −5                         | Canada/Atlantic     | −4                         |
| America/Santiago     | −4                         | Canada/Newfoundland | −3.30                      |
| Atlantic/Azores      | −1                         | Canada/Saskatchewan | −6                         |
| Atlantic/Cape_Verde  | −1                         | Europe/Athens       | +2                         |
| Asia/Almaty          | +6                         | Europe/Berlin       | +1                         |
| Asia/Baghdad         | +3                         | Europe/Bucharest    | +2                         |
| Asia/Baku            | +4                         | Europe/Helsinki     | +2                         |
| Asia/Bangkok         | +7                         | Europe/London       | 0                          |
| Asia/Colombo         | +6                         | Europe/Moscow       | +3                         |
| Asia/Dacca           | +6                         | Europe/Paris        | +1                         |

**Table 5-31** Time Zone—Offset from UTC (continued)

| Time Zone        | Offset from UTC (in hours) | Time Zone         | Offset from UTC (in hours) |
|------------------|----------------------------|-------------------|----------------------------|
| Asia/Hong_Kong   | +8                         | Europe/Prague     | +1                         |
| Asia/Irkutsk     | +8                         | Europe/Warsaw     | +1                         |
| Asia/Jerusalem   | +2                         | Japan             | +9                         |
| Asia/Kabul       | +4.30                      | Pacific/Auckland  | +12                        |
| Asia/Karachi     | +5                         | Pacific/Fiji      | +12                        |
| Asia/Katmandu    | +5.45                      | Pacific/Guam      | +10                        |
| Asia/Krasnoyarsk | +7                         | Pacific/Kwajalein | –12                        |
| Asia/Magadan     | +11                        | Pacific/Samoa     | –11                        |
| Asia/Muscat      | +4                         | US/Alaska         | –9                         |
| Asia/New Delhi   | +5.30                      | US/Central        | –6                         |
| Asia/Rangoon     | +6.30                      | US/Eastern        | –5                         |
| Asia/Riyadh      | +3                         | US/East–Indiana   | –5                         |
| Asia/Seoul       | +9                         | US/Hawaii         | –10                        |
| Asia/Singapore   | +8                         | US/Mountain       | –7                         |
| Asia/Taipei      | +8                         | US/Pacific        | –8                         |
| Asia/Tehran      | +3.30                      | —                 | —                          |

The offset time (number of hours ahead or behind UTC) as displayed in the table is in effect during winter time. During summer time or daylight savings time, the offset may be different from the values in the table and is calculated and displayed accordingly by the system clock.

## Viewing Network Interfaces

The Network Interfaces page is informational only. To view this information, choose **Devices > Devices > General Settings > Network > Network Interfaces**. Information about the network interfaces configured for the device is displayed.

## Configuring External IP Addresses

The External IP page allows you to configure up to eight Network Address Translation (NAT) IP addresses. This allows a router to translate up to eight internal addresses to registered unique addresses and translate external registered addresses to addresses that are unique to the private network.

To configure NAT IP addresses:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Network > External IP**. The External IP Settings page is displayed.
  - Step 5** Check the **Enable** check box.

- Step 6** In the External IP Address fields (1–8), enter up to eight IP addresses.
- Step 7** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Configuring Port Channel and Load Balancing Settings

To configure load balancing on port channels:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Network > Port Channel Settings**. The Port Channel Settings page is displayed.
- Step 5** From the **Load Balancing Method** drop-down list, choose one of the following load balancing methods:
- **dst-ip**—Destination IP address
  - **dst-mac**—Destination MAC address
  - **dst-port**—Destination port
  - **round robin**—Each interface in the channel group
  - **src-dst-mac**—Source and destination MAC address
  - **src-dst-port**—Source and destination port
  - **src-port**—Source port

Round robin allows traffic to be distributed evenly among all interfaces in the channel group. The other balancing options give you the flexibility to choose specific interfaces (by IP address, MAC address, port) when sending an Ethernet frame.

The source and destination options means, while calculating the outgoing interface, take into account both the source and destination (MAC address or port).

- Step 6** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Configuring IP General Settings

The Path Maximum Transmission Unit (MTU) Discovery discovers the largest IP packet size allowable between the various links along the forwarding path and automatically sets the correct value for the packet size. By using the largest MTU the links can support, the sending device can minimize the number of packets it must send.

**Note**

The Path MTU Discovery is a process initiated by the sending device. If a server does not support IP Path MTU Discovery, the receiving device has no mechanism available to avoid fragmenting datagrams generated by the server.

To enable Path MTU Discovery:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Network > IP General Settings**. The IP General Settings page is displayed.
  - Step 5** Check **Enable Path MTU Discovery**.
  - Step 6** Click **Submit** to save the settings.
    - To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
    - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Configuring IP ACL

**Note**

If your system is configured for WCCP, skip this section; IP ACLs are not supported with WCCP.

See the following sections:

- [About IP ACL, page 5-84](#)
- [Creating a New IP ACL, page 5-85](#)
- [Adding Conditions to an IP ACL, page 5-86](#)
- [Applying an IP ACL to an Interface, page 5-92](#)
- [Deleting an IP ACL, page 5-93](#)
- [Checking IP ACL Feature Useage, page 5-93](#)
- [Configuring Static IP Routes, page 5-94](#)
- [Configuring DSR VIP, page 5-95](#)

### About IP ACL

Access control lists (ACLs) provide a means to filter packets by allowing a user to permit or deny IP packets from crossing specified interfaces. Packet filtering helps to control packet movement through the network. Such control can help limit network traffic and restrict network use by certain users or devices.

You can also apply ACLs to management services such as SNMP, SSH, HTTPS, Telnet, and FTP. ACLs can be used to control the traffic that these applications provide by restricting the type of traffic that the applications handle.

In a managed ECDS network environment, administrators need to be able to prevent unauthorized access to various devices and services. ECDS supports standard and extended ACLs that allow administrators to restrict access to or through an ECDS network device, such as the SE. Administrators can use ACLs to reduce the infiltration of hackers, worms, and viruses that can harm the network.

ACLs provide controls that allow various services to be tied to a particular interface. For example, the administrator can use IP ACLs to define a public interface on the Service Engine for content serving and a private interface for management services (for example, Telnet, SSH, SNMP, HTTPS, and software upgrades). A device attempting to access one of the services must be on a list of trusted devices before it is allowed access. The implementation of ACLs for incoming traffic on certain ports for a particular protocol type is similar to the ACL support for the Cisco Global Site Selector and Cisco routers.

To use ACLs, the system administrator must first configure ACLs and then apply them to specific services. The following are some examples of how IP ACLs can be used in various enterprise deployments:

- Application layer proxy firewall with a hardened outside interface has no ports exposed. (*Hardened* means that the interface carefully restricts which ports are available for access primarily for security reasons. Because the interface is outside, many types of attacks are possible.) The device's outside address is globally accessible from the Internet, while its inside address is private. The inside interface has an ACL to limit Telnet, SSH, and CDSM traffic.
- Device is deployed anywhere within the enterprise. Like routers and switches, the administrator wants to limit Telnet, SSH, and CDSM access to the IT source subnets.

**Note**

IP ACLs are defined for individual devices only. IP ACLs cannot be managed through device groups.

When you create an IP ACL, you should note the following constraints:

- IP ACL names must be unique within the device.
- IP ACL names must be limited to 30 characters and contain no spaces or special characters.
- CDSM can manage up to 50 IP ACLs and a total of 500 conditions per device.
- When the IP ACL name is numeric, numbers 1 through 99 denote standard IP ACLs and numbers 100 through 199 denote extended IP ACLs. IP ACL names that begin with a number cannot contain nonnumeric characters.
- Extended IP ACLs cannot be used with SNMP applications.

## Creating a New IP ACL

To create a new IP ACL:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Network > IP ACL**. The IP ACL Table page is displayed.  
The table is sortable by clicking the column headings.
- Step 5** Click the **Create New** icon in the task bar. The IP ACL page is displayed.  
To edit an ACL, click the **Edit** icon next to the name you want to edit.
- Step 6** In the **Name** field, enter a name, observing the naming rules for IP ACLs.

- Step 7** From the **ACL Type** drop-down list, choose an IP ACL type (**Standard** or **Extended**). The default is **Standard**.
- Step 8** Click **Submit**. The page refreshes and the Modifying IP ACL page for a newly created IP ACL is displayed.



**Note** Clicking **Submit** at this point merely saves the IP ACL; IP ACLs without any conditions defined do not appear on the individual devices.

## Adding Conditions to an IP ACL

To add conditions to an IP ACL:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Network > IP ACL**. The IP ACL Table page is displayed.
- Step 5** Click the **Edit** icon next to the name of the IP ACL you want to add a condition to. The Modifying IP ACL page is displayed.
- Step 6** Click the **Create New** icon in the task bar. The Condition page is displayed.

To edit a condition, click the **Edit** icon next to the name you want to edit.



**Note** The number of available fields for creating IP ACL conditions depends on the whether the IP ACL type is standard or extended.

- Step 7** Enter values for the properties that are enabled for the type of IP ACL that you are creating.
- To create a standard IP ACL, go to [Step 8](#).
  - To create an extended IP ACL, go to [Step 9](#).
- Step 8** To set up conditions for a standard IP ACL:
- a. From the **Purpose** drop-down list, choose a purpose (**Permit** or **Deny**).
  - b. In the **Source IP** field, enter the source IP address.
  - c. In the **Source IP Wildcard** field, enter a source IP wildcard address.
  - d. Click **Submit**. The Modifying IP ACL page is displayed showing the new condition and its configuration.
  - e. To add another condition to the IP ACL, repeat the steps.
  - f. To reorder your list of conditions in the Modifying IP ACL page, use the Up arrow or Down arrow in the **Order** column, or click a column heading to sort by any configured parameter.



**Note** The order of the conditions listed becomes the order in which IP ACLs are applied to the device.



- g. When you have finished adding conditions to the IP ACL, and you are satisfied with all your entries and the order in which the conditions are listed, click **Submit** in the Modifying IP ACL page to commit the IP ACL to the device database.

A green “Change submitted” indicator appears in the lower right corner of the Modifying IP ACL page to indicate that the IP ACL is being submitted to the device database.

Table 5-32 describes the fields in a standard IP ACL.

**Table 5-32 Standard IP ACL Conditions**

| Field              | Default Value   | Description                                                                                                                                                                                                         |
|--------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Purpose            | Permit          | Required. Specifies whether a packet is to be passed ( <b>Permit</b> ) or dropped ( <b>Deny</b> ).                                                                                                                  |
| Source IP          | 0.0.0.0         | Required. IP address of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.                                                                    |
| Source IP Wildcard | 255.255.255.255 | Required. Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0. |

**Step 9** To set up conditions for an extended IP ACL:

- a. From the **Purpose** drop-down list, choose a purpose (**Permit** or **Deny**).
- b. From the **Extended Type** drop-down list, choose **Generic**, **TCP**, **UDP**, or **ICMP**.  
After you choose a type of extended IP ACL, various options become available depending on what type you choose.
- c. Enter the settings as appropriate. See Table 5-33 for descriptions of the extended IP ACL fields.
- d. Click **Submit**. The Modifying IP ACL page is displayed showing the new condition and its configuration.
- e. To add another condition to the IP ACL, repeat the steps.
- f. To reorder your list of conditions from the Modifying IP ACL page, use the Up arrow or Down arrow in the **Order** column, or click a column heading to sort by any configured parameter.



**Note** The order of the conditions listed becomes the order in which IP ACLs are applied to the device.

- g. When you have finished adding conditions to the IP ACL, and you are satisfied with all your entries and the order in which the conditions are listed, click **Submit** in the Modifying IP ACL page to commit the IP ACL to the device database.

A green “Change submitted” indicator appears in the lower-left corner of the Modifying IP ACL page to indicate that the IP ACL is being submitted to the device database.

**Table 5-33**      **Extended IP ACL Conditions**

| Field                   | Default Value     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Extended Type           |
|-------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Purpose                 | Permit            | Required. Specifies whether a packet is to be passed ( <b>Permit</b> ) or dropped ( <b>Deny</b> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Generic, TCP, UDP, ICMP |
| Protocol                | ip                | Internet protocol ( <b>gre</b> , <b>icmp</b> , <b>ip</b> , <b>tcp</b> , or <b>udp</b> ). To match any Internet protocol, use the <b>ip</b> keyword.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Generic                 |
| Established             | Unchecked (false) | When checked, a match with the ACL condition occurs if the TCP datagram has the ACK or RST bits set, indicating an established connection. Initial TCP datagrams used to form a connection are not matched.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | TCP                     |
| Source IP               | 0.0.0.0           | Required. IP address of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Generic, TCP, UDP, ICMP |
| Source IP Wildcard      | 255.255.255.255   | Required. Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Generic, TCP, UDP, ICMP |
| Source Port 1           | 0                 | <div>Decimal number or name of a port. Valid port numbers are 0 to 65535. See <a href="#">Table 5-34</a> and <a href="#">Table 5-35</a> for port name descriptions and associated port numbers.</div> <div><div>Valid TCP port names are as follows:</div><div><ul style="list-style-type: none"><li>• domain</li><li>• exec</li><li>• ftp</li><li>• ftp-data</li><li>• https</li><li>• nfs</li><li>• rtsp</li><li>• ssh</li><li>• telnet</li><li>• www</li></ul></div><div>Valid UDP port names are as follows:</div><div><ul style="list-style-type: none"><li>• bootpc</li><li>• bootps</li><li>• domain</li><li>• netbios-dgm</li><li>• netbios-ns</li><li>• netbios-ss</li><li>• nfs</li><li>• ntp</li><li>• snmp</li><li>• snmptrap</li></ul></div></div> | TCP, UDP                |
| Source Operator         | range             | Specifies how to compare the source ports against incoming packets. Choices are <, >, ==, !=, or <b>range</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | TCP, UDP                |
| Source Port 2           | 65535             | Decimal number or name of a port. See Source Port 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | TCP, UDP                |
| Destination IP          | 0.0.0.0           | IP address of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Generic, TCP, UDP, ICMP |
| Destination IP Wildcard | 255.255.255.255   | Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Generic, TCP, UDP, ICMP |

**Table 5-33**      *Extended IP ACL Conditions (continued)*

| Field                | Default Value               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Extended Type |
|----------------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Destination Port 1   | 0                           | <div>Decimal number or name of a port. Valid port numbers are 0 to 65535. See <a href="#">Table 5-34</a> and <a href="#">Table 5-35</a> for port name descriptions and associated port numbers.</div> <div><div>Valid TCP port names are as follows:</div><div><div><ul style="list-style-type: none"><li>• domain</li><li>• exec</li><li>• ftp</li><li>• ftp-data</li><li>• https</li><li>• nfs</li><li>• rtsp</li><li>• ssh</li><li>• telnet</li><li>• www</li></ul></div><div>Valid UDP port names are as follows:</div><div><div><ul style="list-style-type: none"><li>• bootpc</li><li>• bootps</li><li>• domain</li><li>• netbios-dgm</li><li>• netbios-ns</li><li>• netbios-ss</li><li>• nfs</li><li>• ntp</li><li>• snmp</li><li>• snmptrap</li></ul></div></div></div></div> | TCP, UDP      |
| Destination Operator | range                       | Specifies how to compare the destination ports against incoming packets. Choices are <, >, ==, !=, or <b>range</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | TCP, UDP      |
| Destination Port 2   | 65535                       | Decimal number or name of a port. See Destination Port 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | TCP, UDP      |
| ICMP Param Type      | None                        | <div>Required. Choices are <b>None</b>, <b>Type/Code</b>, or <b>Msg</b>.</div> <div><ul style="list-style-type: none"><li>• <b>None</b>—Disables the ICMP Type, Code, and Message fields.</li><li>• <b>Type/Code</b>—Allows ICMP messages to be filtered by ICMP message type and code. Also enables the ability to set an ICMP message code number.</li><li>• <b>Msg</b>—Allows a combination of type and code to be specified using a keyword. Activates the ICMP Message drop-down list. Disables the ICMP Type field.</li></ul></div>                                                                                                                                                                                                                                             | ICMP          |
| ICMP Message         | administratively-prohibited | <div>Required. Allows a combination of ICMP type and code to be specified using a keyword chosen from the drop-down list.</div> <div>See <a href="#">Table 5-36</a> for descriptions of the ICMP messages.</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | ICMP          |
| ICMP Type            | 0                           | Required. Number from 0 to 255. This field is enabled when you choose <b>Type/Code</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | ICMP          |
| Use ICMP Code        | Unchecked                   | Required. When checked, enables the ICMP Code field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | ICMP          |
| ICMP Code            | 0                           | Required. Number from 0 to 255. Message code option that allows ICMP messages of a particular type to be further filtered by an ICMP message code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | ICMP          |

[Table 5-34](#) lists the UDP keywords that you can use with extended access control lists.

**Table 5-34** UDP Keywords and Port Numbers

| Port Name   | Description                                | UDP Port Number |
|-------------|--------------------------------------------|-----------------|
| bootpc      | Bootstrap Protocol (BOOTP) client service  | 68              |
| bootps      | Bootstrap Protocol (BOOTP) server service  | 67              |
| domain      | Domain Name System (DNS) service           | 53              |
| netbios-dgm | NetBIOS datagram service                   | 138             |
| netbios-ns  | NetBIOS name resolution service            | 137             |
| netbios-ss  | NetBIOS session service                    | 139             |
| nfs         | Network File System service                | 2049            |
| ntp         | Network Time Protocol settings             | 123             |
| snmp        | Simple Network Management Protocol service | 161             |
| snmptrap    | SNMP traps                                 | 162             |

Table 5-35 lists the TCP keywords that you can use with extended access control lists.

**Table 5-35** TCP Keywords and Port Numbers

| Port Name | Description                               | TCP Port Number |
|-----------|-------------------------------------------|-----------------|
| domain    | Domain Name System service                | 53              |
| exec      | Remote process execution                  | 512             |
| ftp       | File Transfer Protocol service            | 21              |
| ftp-data  | FTP data connections (used infrequently)  | 20              |
| https     | Secure HTTP service                       | 443             |
| nfs       | Network File System service applications  | 2049            |
| rtsp      | Real-Time Streaming Protocol applications | 554             |
| ssh       | Secure Shell login                        | 22              |
| telnet    | Remote login using Telnet                 | 23              |
| www       | World Wide Web (HTTP) service             | 80              |

Table 5-36 lists the keywords that you can use to match specific ICMP message types and codes.

**Table 5-36** Keywords for ICMP Message Type and Code

| Message                     | Description                                                                        |
|-----------------------------|------------------------------------------------------------------------------------|
| administratively-prohibited | Messages that are administratively prohibited from being allowed access.           |
| alternate-address           | Messages that specify alternate IP addresses.                                      |
| conversion-error            | Messages that denote a datagram conversion error.                                  |
| dod-host-prohibited         | Messages that signify a Department of Defense (DoD) protocol Internet host denial. |
| dod-net-prohibited          | Messages that specify a DoD protocol network denial.                               |

**Table 5-36**      **Keywords for ICMP Message Type and Code (continued)**

| Message                     | Description                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| echo                        | Messages that are used to send echo packets to test basic network connectivity.                                                                                                                                                                                                                                                   |
| echo-reply                  | Messages that are used to send echo reply packets.                                                                                                                                                                                                                                                                                |
| general-parameter-problem   | Messages that report general parameter problems.                                                                                                                                                                                                                                                                                  |
| host-isolated               | Messages that indicate that the host is isolated.                                                                                                                                                                                                                                                                                 |
| host-precedence-unreachable | Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable). This is the most common response. Large numbers of this datagram type on the network are indicative of network difficulties or may be indicative of hostile actions. |
| host-redirect               | Messages that specify redirection to a host.                                                                                                                                                                                                                                                                                      |
| host-tos-redirect           | Messages that specify redirection to a host for type of service-based (ToS) routing.                                                                                                                                                                                                                                              |
| host-tos-unreachable        | Messages that denote that the host is unreachable for ToS-based routing.                                                                                                                                                                                                                                                          |
| host-unknown                | Messages that specify that the host or source is unknown.                                                                                                                                                                                                                                                                         |
| host-unreachable            | Messages that specify that the host is unreachable.                                                                                                                                                                                                                                                                               |
| information-reply           | Messages that contain domain name replies.                                                                                                                                                                                                                                                                                        |
| information-request         | Messages that contain domain name requests.                                                                                                                                                                                                                                                                                       |
| mask-reply                  | Messages that contain subnet mask replies.                                                                                                                                                                                                                                                                                        |
| mask-request                | Messages that contain subnet mask requests.                                                                                                                                                                                                                                                                                       |
| mobile-redirect             | Messages that specify redirection to a mobile host.                                                                                                                                                                                                                                                                               |
| net-redirect                | Messages that are used for redirection to a different network.                                                                                                                                                                                                                                                                    |
| net-tos-redirect            | Messages that are used for redirection to a different network for ToS-based routing.                                                                                                                                                                                                                                              |
| net-tos-unreachable         | Messages that specify that the network is unreachable for the ToS-based routing.                                                                                                                                                                                                                                                  |
| net-unreachable             | Messages that specify that the network is unreachable.                                                                                                                                                                                                                                                                            |
| network-unknown             | Messages that denote that the network is unknown.                                                                                                                                                                                                                                                                                 |
| no-room-for-option          | Messages that specify the requirement of a parameter, but that no room is available for it.                                                                                                                                                                                                                                       |
| option-missing              | Messages that specify the requirement of a parameter, but that parameter is not available.                                                                                                                                                                                                                                        |
| packet-too-big              | Messages that specify that the ICMP packet requires fragmentation but the Do Not Fragment (DF) bit is set.                                                                                                                                                                                                                        |
| parameter-problem           | Messages that signify parameter-related problems.                                                                                                                                                                                                                                                                                 |
| port-unreachable            | Messages that specify that the port is unreachable.                                                                                                                                                                                                                                                                               |
| precedence-unreachable      | Messages that specify that host precedence is not available.                                                                                                                                                                                                                                                                      |
| protocol-unreachable        | Messages that specify that the protocol is unreachable.                                                                                                                                                                                                                                                                           |

**Table 5-36**      **Keywords for ICMP Message Type and Code (continued)**

| Message              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| reassembly-timeout   | Messages that specify a timeout during reassembling of packets.                                                                                                                                                                                                                                                                                                                                                                                            |
| redirect             | Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect). ICMP redirect messages are used by routers to notify the hosts on the data link that a better route is available for a particular destination.                                                                                                                                                        |
| router-advertisement | Messages that contain ICMP router discovery messages called router advertisements.                                                                                                                                                                                                                                                                                                                                                                         |
| router-solicitation  | Messages that are multicast to ask for immediate updates on neighboring router interface states.                                                                                                                                                                                                                                                                                                                                                           |
| source-quench        | Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench). This datagram may be used in network management to provide congestion control. A source quench packet is issued when a router is beginning to lose packets due to the transmission rate of a source. The source quench is a request to the source to reduce the rate of a datagram transmission. |
| source-route-failed  | Messages that specify the failure of a source route.                                                                                                                                                                                                                                                                                                                                                                                                       |
| time-exceeded        | Messages that specify information about all instances when specified times were exceeded.                                                                                                                                                                                                                                                                                                                                                                  |
| timestamp-reply      | Messages that contain timestamp replies.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| timestamp-request    | Messages that contain timestamp requests.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| traceroute           | Messages that specify the entire route to a network host from the source.                                                                                                                                                                                                                                                                                                                                                                                  |
| ttl-exceeded         | Messages that specify that ICMP packets have exceeded the time-to-live configuration.                                                                                                                                                                                                                                                                                                                                                                      |
| unreachable          | Messages that are sent when packets are denied by an access control list; these packets are not dropped in the hardware but generate the ICMP-unreachable message.                                                                                                                                                                                                                                                                                         |

## Applying an IP ACL to an Interface

The IP ACLs can be applied to a particular interface (such as management services to a private IP address) so that the device can have one interface in a public IP address space that serves content and another interface in a private IP address space that the administrator uses for management purposes. This feature ensures that clients can access the Service Engine only in the public IP address space for serving content and not access it for management purposes. A device attempting to access one of these applications that is associated with an IP ACL must be on the list of trusted devices to be allowed access.

To apply an IP ACL to an interface from the CLI, use the following interface configuration command:

```
interface {FastEthernet | GigabitEthernet} slot/port ip access-group {accesslistnumber | accesslistname} {in | out}
```

## Deleting an IP ACL

You can delete an IP ACL, including all conditions and associations with network interfaces, or you can delete only the IP ACL conditions. Deleting all conditions allows you to change the IP ACL type if you choose to do so. The IP ACL entry continues to appear in the IP ACL listing; however, it is in effect nonexistent.

To delete an IP ACL:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Network > IP ACL**. The IP ACL Table page is displayed.
  - Step 5** Click the **Edit** icon next to the name of the IP ACL that you want to delete. The Modifying IP ACL page is displayed. If you created conditions for the IP ACL, you have three options for deletion:
    - **Delete ACL**—This option removes the IP ACL, including all conditions and associations with network interfaces and applications.
    - **Delete All Conditions**—This option removes all the conditions, while preserving the IP ACL name.
    - **Delete IP ACL Condition**—This option removes one condition from the ACL.
  - Step 6** To delete the entire IP ACL, click **Delete ACL** in the task bar. You are prompted to confirm your action. Click **OK**. The record is deleted.
  - Step 7** To delete only the conditions, click **Delete All Conditions** in the task bar. You are prompted to confirm your action. Click **OK**. The window refreshes, conditions are deleted, and the ACL Type field becomes available.
  - Step 8** To delete one condition:
    - a. Click the **Edit** icon next to the condition. The condition settings are displayed.
    - b. Click the **Delete IP ACL Condition** icon in the task bar. The IP ACL table is displayed.
    - c. Click **Submit** to save the IP ACL table to the database.
- 

## Checking IP ACL Feature Usage

There is no IP ACL feature usage support at this time for systems using WCCP; support is expected in the future. This option is not available for systems prior to Cisco ECDS Software Release 2.5.5 without WCCP.

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Network > IP ACL Feature Usage**. The IP ACL Feature Settings for Service Engine page is displayed, as shown in [Figure 5-29](#).

**Figure 5-29** IP ACL Feature Usage

The screenshot displays the 'IP ACL Feature Settings' configuration page. The left sidebar contains a navigation menu with categories like 'Authentication', 'Database Maintenance', 'Storage', 'Network', 'Notification and Tracking', 'Troubleshooting', 'Service Router Settings', and 'Monitoring'. Under 'Network', 'IP ACL Feature Usage' is selected. The main content area shows the 'IP ACL Feature Settings' for Service Engine, cc-se1125. A 'WCCP' field is present with a dropdown menu currently set to 'Do Not Set'. A note below the field states 'Note: \* - Required Field'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

**Step 5** If you are using WCCP, no features are available from the drop-down menu.

## Configuring Static IP Routes

The Static IP Routes page allows you to configure a static route for a network or host. Any IP packet designated for the specified destination uses the configured route.

To configure a static IP route:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Network > IP Routes**. The IP Route Table page is displayed.  
The table is sortable by clicking the column headings.
- Step 5** Click the **Create New** icon in the task bar. The IP Route page is displayed.  
To edit a static route, click the **Edit** icon next to the name you want to edit.
- Step 6** In the **Destination Network Address** field, enter the destination network IP address.
- Step 7** In the **Netmask** field, enter the destination host netmask.
- Step 8** In the **Gateway's IP Address** field, enter the IP address of the gateway interface.
- Step 9** Click **Submit** to save the settings.

To delete a route, click the **Edit** icon for the route, then click the **Delete** icon in the task bar.



## Configuring DSR VIP

The ECDS supports Virtual IP (VIP) configuration for Direct Server Return (DSR) when working with networks that use load balancers. DSR bypasses the load balancer for all server responses to client requests by using MAC Address Translation (MAT).

The ECDS allows for the configuration of up to four VIPs (on loopback interfaces).

Client requests are sent to the load balancer and the load balancer sends the requests on to the Service Router. If DSR VIP is configured on the ECDS (and supported on the load balancer), all ECDS responses to the client are sent directly to the client, bypassing the load balancer.

To configure a DSR VIP:

- 
- |               |                                                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Devices &gt; Devices</b> . The Devices Table page is displayed.                                                                                                                                                                                                                                        |
| <b>Step 2</b> | Click the <b>Edit</b> icon next to the device you want to configure. The Devices home page is displayed.                                                                                                                                                                                                         |
| <b>Step 3</b> | Click <b>Show All</b> to display the top-level menu options.                                                                                                                                                                                                                                                     |
| <b>Step 4</b> | Choose <b>General Settings &gt; Network &gt; DSR VIP</b> . The DSR VIP page is displayed.                                                                                                                                                                                                                        |
| <b>Step 5</b> | In the <b>Direct Server Return VIP 1</b> field, enter the IP address of the Direct Server Return VIP.                                                                                                                                                                                                            |
| <b>Step 6</b> | Enter any additional DSR VIPs in the remaining fields (Direct Server Return VIP 2 to 4).                                                                                                                                                                                                                         |
| <b>Step 7</b> | Click <b>Submit</b> to save the settings. <ul style="list-style-type: none"><li>• To apply the factory default settings for the device, click the <b>Apply Defaults</b> icon in the task bar.</li><li>• To remove the settings from the device, click the <b>Remove Settings</b> icon in the task bar.</li></ul> |
- 

## Configuring Notification and Tracking

The Notification and Tracking pages provide settings for alarms, thresholds, SNMP connectivity, and device monitoring. Configuring notification and tracking consists of the following procedures:

- [Enabling Alarm Settings, page 5-95](#)
- [Setting Service Monitor Thresholds, page 5-97](#)
- [Configuring SNMP, page 5-100](#)
- [Enabling System Logs, page 5-107](#)

### Enabling Alarm Settings

The device tracks the rate of incoming alarms from the Node Health Manager. If the rate of incoming alarms exceeds the high-water mark (HWM) threshold, the device enters an alarm overload state. This condition occurs when multiple applications raise alarms at the same time. When a device is in an alarm overload state, the following events occur:

- Traps for the raise alarm-overload alarm and clear alarm-overload alarm are sent. SNMP traps for subsequent alarm raise-and-clear operations are suspended.
- Traps for alarm operations that occur between the raise-alarm-overload alarm and the clear-alarm-overload alarm operations are suspended, but individual device alarm information is still collected and available using the CLI.

- Device remains in an alarm overload state until the rate of incoming alarms decreases to less than the low-water mark (LWM).
- If the incoming alarm rate falls below the LWM, the device comes out of the alarm overload state and begins to report the alarm counts to the SNMP servers and the CDSM.

Alarms that have been raised on a device can be listed by using the CLI commands shown in [Table 5-37](#). These CLI commands allow you to systematically drill down to the source of an alarm.

**Table 5-37 Show Alarms Command**

| Command            | Syntax                      | Description                                                                                                                                   |
|--------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show alarms</b> |                             | Displays a list of all currently raised alarms (critical, major, and minor alarms) on the device.                                             |
|                    | <b>show alarms critical</b> | Displays a list of only currently raised critical alarms on the device.                                                                       |
|                    | <b>show alarms major</b>    | Displays a list of only currently raised major alarms on the device.                                                                          |
|                    | <b>show alarms minor</b>    | Displays a list of only currently raised minor alarms on the device.                                                                          |
|                    | <b>show alarms detail</b>   | Displays detailed information about the currently raised alarms.                                                                              |
|                    | <b>show alarms history</b>  | Displays a history of alarms that have been raised and cleared on the device. The CLI retains the last 100 alarm raise and clear events only. |
|                    | <b>show alarms status</b>   | Displays the counts for the currently raised alarms on the device. Also lists the alarm-overload state and the alarm-overload settings.       |

#### Procedure

To configure alarm overload detection:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Notification and Tracking > Alarm Settings**. The Alarm Settings on Service Engine page is displayed.
- Step 5** Uncheck the **Enable Alarm Overload Detection** check box if you do not want to configure the device to suspend alarm raise and clear operations when multiple applications report error conditions. Alarm overload detection is enabled by default.
- Step 6** In the **Alarm Overload Low Water Mark** field, enter the number of alarms per second for the clear alarm overload threshold. The low water mark is the level to which the number of alarms must drop below before alarm traps can be sent. The default value is 1.
- Step 7** In the **Alarm Overload High Water Mark** field, enter the number of alarms per second for the raise alarm-overload threshold. The high-water mark is the level the number of alarms must exceed before alarms are suspended. The default value is 10.
- Step 8** In the Alarm Generation section, check the **Alarms for Interface Shutdown** box to enable NIC alarm reporting. By default, the minor alarm, Network Interface Controller (NIC) shutdown, is not displayed in either the **show alarms** command output or in CDSM reporting.  
Use the **alarm nic-shutdown enable** command.

**Tip**

After configuring the setting, you may need to wait a few minutes before the alarm is shown in **show alarms** output.

**Step 9** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Setting Service Monitor Thresholds

The Service Monitor page is where you configure workload thresholds for the device. In load-based routing, these thresholds are used to determine the best device to serve requested content. For more information about load-based routing, see the [“Configuring the Service Router” section on page 6-1](#).

### Before You Begin

Observe the following:

- Threshold monitoring is performed on each device in the ECDS. The protocol engine and NIC bandwidth thresholds are only monitored on the SE. They are not monitored on the SR or CDSM.
- Sample period and number of samples are not required for Movie Streamer and Web Engine because these protocol engines do not support bandwidth-based threshold monitoring.
- System overload threshold for transparent routing with WCCP behaves differently than service routing without WCCP:
  - During overload status in a system enabled with WCCP, the Service Engine bypasses new WCCP requests and continues to serve existing requests until a specified (configurable) amount of time or until the overload status is relieved.
  - For service routing on systems that are not using WCCP, the Service Router assigns traffic to other Service Engines, if applicable.:

### Procedure

To configure workload thresholds:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Notification and Tracking > Service Monitor**. The Service Monitor page is displayed.
- Step 5** Enter the settings as appropriate. See [Table 5-38](#) for a description of the fields.

**Table 5-38** Service Monitor Fields

| Field               | Description                                                    |
|---------------------|----------------------------------------------------------------|
| <b>CPU Settings</b> |                                                                |
| Enable              | Allows the SR to collect CPU load information from the device. |

**Table 5-38 Service Monitor Fields (continued)**

| Field                   | Description                                                                                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threshold               | Value (as a percentage) that determines when the device is overloaded. The threshold determines the extent of CPU usage allowed. The range is from 1 to 100. The default is 80.                                                                  |
| Sample Period           | Time interval (in seconds) between two consecutive samples. The sample period is the time during which the device and the SR exchange keep-alive messages that contain the device load information. The range is from 1 to 60. The default is 1. |
| Number of Samples       | Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.                                                                                                                          |
| <b>Disk Settings</b>    |                                                                                                                                                                                                                                                  |
| Enable                  | Allows the SR to collect disk transaction information from the device.                                                                                                                                                                           |
| Threshold               | The threshold, as a percentage, determines the extent of disk I/O access allowed. The range is from 1 to 100. The default is 80.                                                                                                                 |
| Sample Period           | Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.                                                                                                                                         |
| Number of Samples       | Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.                                                                                                                          |
| <b>Memory Settings</b>  |                                                                                                                                                                                                                                                  |
| Enable                  | Allows the SR to collect memory usage information from the device.                                                                                                                                                                               |
| Threshold               | The threshold (in percent) determines the extent of memory usage allowed. The range is from 1 to 100. The default is 80.                                                                                                                         |
| Sample Period           | Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.                                                                                                                                         |
| Number of Samples       | Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.                                                                                                                          |
| <b>KMemory Settings</b> |                                                                                                                                                                                                                                                  |
| Enable                  | Allows the SR to collect kernel memory usage information from the device.                                                                                                                                                                        |
| Threshold               | The threshold (in percent) determines the extent of kernel memory usage allowed. The range is from 1 to 100. The default is 50.                                                                                                                  |
| Sample Period           | Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.                                                                                                                                         |
| Number of Samples       | Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.                                                                                                                          |
| <b>WMT Settings</b>     |                                                                                                                                                                                                                                                  |
| Enable                  | Allows the SR to collect Windows Media Streaming stream count information from the SE.                                                                                                                                                           |
| Threshold               | Percentage of streams for which the SE has been either configured or licensed. The range is from 1 to 100. The default is 90.                                                                                                                    |
| Sample Period           | Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.                                                                                                                                         |
| Number of Samples       | Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.                                                                                                                          |

**Table 5-38 Service Monitor Fields (continued)**

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FMS Settings</b>                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Enable                             | Allows the SR to collect Flash Media Streaming stream count information from the SE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Threshold                          | Percentage of streams for which the SE has been either configured or licensed. The range is from 1 to 100. The default is 90.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Sample Period                      | Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Number of Samples                  | Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Movie Streamer Settings</b>     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Enable                             | Allows the SR to collect stream count information from the SE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Threshold                          | Percentage of streams for which the SE has been either configured or licensed. The range is from 1 to 100. The default is 90.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Web Engine Settings</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Enable                             | Allows the SR to collect stream count information from the SE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Threshold                          | Percentage of streams for which the SE has been either configured or licensed. The range is from 1 to 100. The default is 90.<br><br>We recommend setting the Web Engine Threshold to 80 percent or higher when Flash Media Streaming is enabled.                                                                                                                                                                                                                                                                                                                                                    |
| <b>NIC Bandwidth Settings</b>      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Enable                             | Allows the SR to collect NIC bandwidth information from the SE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Threshold                          | The threshold, as a percentage, determines the extent of NIC bandwidth usage allowed. The range is from 1 to 100. The default is 90.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Sample Period                      | Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Number of Samples                  | Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Disk Failure Count Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Threshold                          | When the number of failed disks exceeds this threshold, no further requests are sent to this device. The Disk Failure Count Threshold is only for the CDNFS disks. The maximum threshold that can be configured is determined by the physical number of CDNFS disks (up to 15) installed on the device. The default is 1.<br><br><b>Note</b> When an alarm is received for a SYSFS disk, it is immediately marked as a failed disk. It is not checked against the Disk Failure Count Threshold. The SR continues redirecting to the SE, unless all SYSFS disks on the SE are marked as failed disks. |

**Step 6** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Configuring SNMP

The Cisco ECDS supports the following versions of SNMP:

- Version 1 (SNMPv1)—A network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
- Version 2 (SNMPv2c)—The second version of SNMP, it supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.
- Version 3 (SNMPv3)—An interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:
  - Message integrity—Ensuring that a packet has not been tampered with in-transit.
  - Authentication—Determining the message is from a valid source.
  - Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

Table 5-39 identifies what the combinations of security models and levels mean.

**Table 5-39** *SNMP Security Models and Levels*

| Model | Level        | Authentication   | Encryption | Process                                                                                                                                                                    |
|-------|--------------|------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| v1    | noAuthNoPriv | Community String | No         | Uses a community string match for authentication.                                                                                                                          |
| v2c   | noAuthNoPriv | Community String | No         | Uses a community string match for authentication.                                                                                                                          |
| v3    | noAuthNoPriv | Username         | No         | Uses a username match for authentication.                                                                                                                                  |
| v3    | authNoPriv   | MD5 or SHA       | No         | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.                                                                                                      |
| v3    | authPriv     | MD5 or SHA       | DES        | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. |

The SNMPv3 agent can be used in the following modes:

- noAuthNoPriv mode (that is, no security mechanisms turned on for packets)
- AuthNoPriv mode (for packets that do not need to be encrypted using the privacy algorithm [DES 56])
- AuthPriv mode (for packets that must be encrypted; privacy requires that authentication be performed on the packet)

Using SNMPv3, users can securely collect management information from their SNMP agents without worrying that the data has been tampered with. Also, confidential information, such as SNMP set packets that change a Service Engine's configuration, can be encrypted to prevent their contents from being exposed on the wire. Also, the group-based administrative model allows different users to access the same SNMP agent with varying access privileges.

Note the following about SNMPv3 objects:

- Each user belongs to a group.
- Group defines the access policy for a set of users.
- Access policy is what SNMP objects can be accessed for reading, writing, and creating.
- Group determines the list of notifications its users can receive.
- Group also defines the security model and security level for its users.

#### Procedure

To configure the SNMP settings:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Notification and Tracking > SNMP > General Settings**. The SNMP General Settings page is displayed.
- Step 5** Enable the settings as appropriate. See [Table 5-40](#) for a description of the fields.

**Table 5-40** *SNMP General Settings Fields*

| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Traps</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Enable SNMP Settings | Enables the SNMP agent to transmit traps to the SNMP server.                                                                                                                                                                                                                                                                                                                                                        |
| Service Engine       | Enables the Disk Fail trap, which is the disk failure error trap.                                                                                                                                                                                                                                                                                                                                                   |
| SNMP                 | Enables SNMP-specific traps: <ul style="list-style-type: none"> <li>• Authentication—Enables authentication trap.</li> <li>• Cold Start—Enables cold start trap.</li> </ul>                                                                                                                                                                                                                                         |
| SE Alarm             | Enables alarm traps: <ul style="list-style-type: none"> <li>• Raise Critical—Enables raise-critical alarm trap.</li> <li>• Clear Critical—Enables clear-critical alarm trap.</li> <li>• Raise Major—Enables raise-major alarm trap.</li> <li>• Clear Major—Enables clear-major alarm trap.</li> <li>• Raise Minor—Enables raise-minor alarm trap.</li> <li>• Clear Minor—Enables clear-minor alarm trap.</li> </ul> |
| Entity               | Enables SNMP entity traps.                                                                                                                                                                                                                                                                                                                                                                                          |
| Config               | Enables CiscoConfigManEvent error traps.                                                                                                                                                                                                                                                                                                                                                                            |

**Table 5-40** *SNMP General Settings Fields (continued)*

| Field                         | Description                             |
|-------------------------------|-----------------------------------------|
| <b>Miscellaneous Settings</b> |                                         |
| Notify Inform                 | Enables the SNMP notify inform request. |

- Step 6** Click **Submit** to save the settings.
- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
  - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- Step 7** From the left-panel menu, click **Community**. The SNMP Community Table page is displayed.
- The table is sortable by clicking the column headings. The maximum number of community strings that can be created is ten.
- Step 8** Click the **Create New** icon in the task bar. The SNMP Community page is displayed.
- Click the **Edit** icon next to the community name to edit a community setting.
- Step 9** Enter the settings as appropriate. See [Table 5-41](#) for a description of the fields.

**Table 5-41** *SNMP Community Fields*

| Field         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Community     | Community string used as a password for authentication when you access the SNMP agent of the device using SNMPv1 or SNMPv2. The “Community Name” field of any SNMP message sent to the device must match the community string defined here to be authenticated. You can enter a maximum of 64 characters in this field.                                                                                                                                                                                                                                                                                                                                                                                 |
| Group name/rw | Group to which the community string belongs. The <b>Read/Write</b> option allows a read or write group to be associated with this community string. The <b>Read/Write</b> option permits access to only a portion of the MIB subtree. Choose one of the following three options from the drop-down list: <ul style="list-style-type: none"> <li><b>None</b>—Choose this option if you do not want to specify a group name to be associated with the community string.</li> <li><b>Read/Write</b>—Choose this option if you want to allow read-write access to the group associated with this community string.</li> <li><b>Group</b>—Choose this option if you want to specify a group name.</li> </ul> |
| Group Name    | Name of the group to which the community string belongs. You can enter a maximum of 64 characters in this field. This field is available only if you have chosen the <b>Group</b> option in the Group name/rw field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

- Step 10** Click **Submit** to save the settings.
- To delete an SNMP community, click the **Edit** icon for the community, then click the **Delete** icon in the task bar.
- Step 11** From the left-panel menu, click **Group**. The SNMP Group Table page is displayed.
- The table is sortable by clicking the column headings. The maximum number of groups that can be created is ten.
- Step 12** Click the **Create New** icon in the task bar. The SNMP Group page is displayed.



Click the **Edit** icon next to the Group Name to edit a group.

**Step 13** Enter the settings as appropriate. See [Table 5-42](#) for a description of the fields.

**Table 5-42** *SNMP Group Fields*

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | <p>Name of the SNMP group. You can enter a maximum of 256 characters.</p> <p>A group defines a set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define what SNMP objects can be read, written to, or created. In addition, the group defines what notifications a user is allowed to receive.</p> <p>An SNMP group is a collection of SNMP users that belong to a common SNMP list that defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of the attributes defined by the group.</p>                                                                                                                                                                                                                                                                                                                                                         |
| Sec Model   | <p>Security model for the group. Choose one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li><b>v1</b>—Version 1 security model (SNMP Version 1 [noAuthNoPriv]).</li> <li><b>v2c</b>—Version 2c security model (SNMP Version 2 [noAuthNoPriv]).</li> <li><b>v3-auth</b>—User security level SNMP Version 3 (AuthNoPriv).</li> <li><b>v3-noauth</b>—User security level SNMP Version 3 (noAuthNoPriv).</li> <li><b>v3-priv</b>—User security level SNMP Version 3 (AuthPriv).</li> </ul> <p>The <b>Sec Model</b> you choose determines which of the following three security algorithms is used on each SNMP packet:</p> <ul style="list-style-type: none"> <li><b>noAuthNoPriv</b>—Authenticates a packet by a string match of the username.</li> <li><b>AuthNoPriv</b>—Authenticates a packet by using either the HMAC MD5 or SHA algorithms.</li> <li><b>AuthPriv</b>—Authenticates a packet by using either the HMAC MD5 or SHA algorithms and encrypts the packet using the CBC-DES (DES-56) algorithm.</li> </ul> |
| Read View   | <p>Name of the view (a maximum of 64 characters) that enables you only to view the contents of the agent. By default, no view is defined. To provide read access to users of the group, a view must be specified.</p> <p>A read view defines the list of object identifiers (OIDs) that are accessible for reading by users belonging to the group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Write View  | <p>Name of the view (a maximum of 64 characters) that enables you to enter data and configure the contents of the agent. By default, no view is defined.</p> <p>A write view defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Notify View | <p>Name of the view (a maximum of 64 characters) that enables you to specify a notify, inform, or trap. By default, no view is defined.</p> <p>A notify view defines the list of notifications that can be sent to each user in the group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Step 14** Click **Submit** to save the settings.

To delete an SNMP group, click the **Edit** icon for the group, then click the **Delete** icon in the task bar.

**Step 15** From the left-panel menu, click **User**. The SNMP User Table page is displayed.

The table is sortable by clicking the column headings. The maximum number of users that can be created is ten.

**Step 16** Click the **Create New** icon in the task bar. The SNMP User page is displayed.

Click the **Edit** icon next to the username to edit a user.

**Step 17** Enter the settings as appropriate. See [Table 5-43](#) for a description of the fields.

**Table 5-43** *SNMP User Fields*

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                     | String representing the name of the user (256 characters maximum) who can access the device.<br><br>An SNMP user is a person for which an SNMP management operation is performed.                                                                                                                                                                                                                                                                                                                                                                                            |
| Group                    | Name of the group (256 characters maximum) to which the user belongs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Remote SNMP ID           | Globally unique identifier for a remote SNMP entity. To send an SNMPv3 message to the device, at least one user with a remote SNMP ID must be configured on the device. The SNMP ID must be entered in octet string format. For example, if the IP address of a remote SNMP entity is 192.147.142.129, then the octet string would be 00:00:63:00:00:00:a1:c0:93:8e:81.                                                                                                                                                                                                      |
| Authentication Algorithm | Authentication algorithm that ensures the integrity of SNMP packets during transmission. Choose one of the following three options from the drop-down list: <ul style="list-style-type: none"> <li>• <b>No-auth</b>—Requires no security mechanism to be turned on for SNMP packets.</li> <li>• <b>MD5</b>—Provides authentication based on the hash-based Message Authentication Code Message Digest 5 (HMAC-MD5) algorithm.</li> <li>• <b>SHA</b>—Provides authentication based on the hash-based Message Authentication Code Secure Hash (HMAC-SHA) algorithm.</li> </ul> |
| Authentication Password  | String (256 characters maximum) that configures the user authentication (HMAC-MD5 or HMAC-SHA) password. The number of characters is adjusted to fit the display area if it exceeds the limit for display.<br><br>This field is optional if the <b>no-auth</b> option is chosen for the authentication algorithm. Otherwise, this field must contain a value.                                                                                                                                                                                                                |
| Confirmation Password    | Authentication password for confirmation. The re-entered password must be the same as the one entered in the Authentication Password field.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Private Password         | String (256 characters maximum) that configures the authentication (HMAC-MD5 or HMAC-SHA) parameters to enable the SNMP agent to receive packets from the SNMP host. The number of characters is adjusted to fit the display area if it exceeds the limit for display.                                                                                                                                                                                                                                                                                                       |
| Confirmation Password    | Private password for confirmation. The re-entered password must be the same as the one entered in the Private Password field.                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Step 18** Click **Submit** to save the settings.

To delete an SNMP user, click the **Edit** icon for the user, then click the **Delete** icon in the task bar.

- Step 19** To define a SNMPv2 MIB view, click **View** from the left-panel menu. The SNMP View Table page is displayed.
- The table is sortable by clicking the column headings. The maximum number of SNMPv2 views that can be created is ten.
- SNMP view—A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.
- Step 20** Click the **Create New** icon in the task bar. The SNMP View page is displayed.
- Click the **Edit** icon next to the username to edit a view.
- Step 21** Enter the settings as appropriate. See [Table 5-44](#) for a description of the fields.

**Table 5-44** *SNMP View Fields*

| Field     | Description                                                                                                                                                                                                                                                                                                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name      | String representing the name of this family of view subtrees (256 characters maximum). The family name must be a valid MIB name such as ENTITY-MIB.                                                                                                                                                                                   |
| Family    | Object identifier (256 characters maximum) that identifies a subtree of the MIB.                                                                                                                                                                                                                                                      |
| View Type | View option that determines the inclusion or exclusion of the MIB family from the view. Choose one of the following two options from the drop-down list: <ul style="list-style-type: none"> <li><b>Included</b>—The MIB family is included in the view.</li> <li><b>Excluded</b>—The MIB family is excluded from the view.</li> </ul> |

- Step 22** Click **Submit** to save the settings.
- To delete an SNMP view, click the **Edit** icon for the view, then click the **Delete** icon in the task bar.
- Step 23** From the left-panel menu, click **Host**. The SNMP Host Table page is displayed.
- The table is sortable by clicking the column headings. The maximum number of hosts that can be created is four.
- Step 24** Click the **Create New** icon in the task bar. The SNMP Host page is displayed.
- Click the **Edit** icon next to the hostname to edit a host.
- Step 25** Enter the settings as appropriate. See [Table 5-45](#) for a description of the fields.

**Table 5-45** *SNMP Host Fields*

| Field          | Description                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------|
| Trap Host      | Hostname or IP address an SNMP entity to which notifications (traps and informs) are to be sent.                |
| Community/User | Name of the SNMP community or user (256 characters maximum) that is sent in SNMP trap messages from the device. |

**Table 5-45** *SNMP Host Fields (continued)*

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication | Security model to use for sending notification to the recipient of an SNMP trap operation. Choose one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>• <b>No-auth</b>—Sends notification without any security mechanism.</li> <li>• <b>v2c</b>—Sends notification using Version 2c security.</li> <li>• <b>Model v3-auth</b>—Sends notification using SNMP Version 3 (AuthNoPriv).</li> <li>• <b>Security Level v3-noauth</b>—Sends notification using SNMP Version 3 (NoAuthNoPriv security).</li> <li>• <b>Level v3-priv</b>—Sends notification using SNMP Version 3 (AuthPriv security).</li> </ul> |
| Retry          | Number of retries (1 to 10) allowed for the inform request. The default is 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Timeout        | Timeout for the inform request in seconds (1 to 1000). The default is 15.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Step 26** Click **Submit** to save the settings.

To delete an SNMP host, click the **Edit** icon for the host, then click the **Delete** icon in the task bar.

**Step 27** From the left-panel menu, click **Asset Tag**. The SNMP Asset Tag page is displayed.

**Step 28** In the **Asset Tag Name** field, enter a name for the asset tag and click **Submit**.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

**Step 29** From the left-panel menu, click **Contact**. The SNMP Contact page is displayed.

**Step 30** In the **Contact** field, enter a name of the contact person for this device.

**Step 31** In the **Location** field, enter a location of the contact person for this device.

**Step 32** Click **Submit** to save the settings.

- To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
- To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Supported MIBs

The SNMP agent supports the following MIBs:

- ENTITY-MIB (RFC 2037 Revision 199610310000Z))
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790, hrSWInstalled and hrPrinterTable subgroups are not supported)
- CISCO-ENTITY-ASSET-MIB
- CISCO-CONFIG-MAN-MIB (Revision 9511280000Z)
- CISCO-SERVICE-ENGINE-MIB (supports streaming media-related MIB objects)

ENTITY-MIB, MIB-II, and HOST-RESOURCES-MIB are public-available MIBs.

The CISCO-SERVICE-ENGINE-MIB is extended to incorporate MIB objects related to streaming. The WMT and Movie Streamer groups incorporate statistics about the WMT server or proxy, and Movie Streamer. The Flash Media Streaming group incorporates statistics about the Flash Media Streaming protocol engine. For each 64-bit counter MIB object, a 32-bit counter MIB object is implemented so that SNMP clients using SNMPv1 can retrieve data associated with 64-bit counter MIB objects. The MIB objects of each of these groups are read-only.

- WMT MIB group provides statistics about WMT proxy and server performance. Twenty-eight MIB objects are implemented in this group. Six of these MIB objects are implemented as 64-bit counters.
- Movie Streamer MIB group provides statistics about RTSP streaming engine performance. Seven MIB objects are implemented in this group. Two of these MIB objects are implemented as 64-bit counters.
- Flash Media Streaming MIB group provides statistics about HTTP and RTMP streaming engine performance.

Use the following link to access the CISCO-ENTITY-ASSET-MIB and the CISCO-CONFIG-MAN-MIB:

<ftp://ftp.cisco.com/pub/mibs/v2/>



#### Note

If your browser is located behind a firewall or you are connecting to the Internet with a DSL modem and you are unable to access this file folder, you must change your web browser compatibility settings. In the Internet Explorer (IE) web browser, choose **Tools > Internet Options > Advanced**, and check the **Use Passive FTP** check box.

To download additional Cisco MIB files, go to the [Support Tools and Resources](#) home page on Cisco.com and click **SNMP Object Navigator**.

## Enabling System Logs

Use the System Logs page to set specific parameters for the system log file (syslog). This file contains authentication entries, privilege level settings, and administrative details. System logging is always enabled. By default, the system log file is stored as /local1/syslog.txt.

To enable system logging:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Notification and Tracking > System Logs**. The System Log Settings page is displayed.
- Step 5** Enter the settings as appropriate. See [Table 5-46](#) for a description of the fields.

**Table 5-46 System Logs Settings Fields**

| Field              | Description                            |
|--------------------|----------------------------------------|
| <b>System Logs</b> |                                        |
| Enable             | Enables system logs.                   |
| Facility           | Facility where the system log is sent. |

**Table 5-46 System Logs Settings Fields (continued)**

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Console Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Enable                  | Enable sending the system log to the console.                                                                                                                                                                                                                                                                                                                                                                             |
| Priority                | Severity level of the message that should be sent to the specified remote syslog host. The default priority is warning. The priorities are:<br>Emergency—System is unusable.<br>Alert—Immediate action needed.<br>Critical—Critical condition.<br>Error—Error conditions.<br>Warning—Warning conditions.<br>Notice—Normal but significant conditions.<br>Information—Informational messages.<br>Debug—Debugging messages. |
| <b>Disk Settings</b>    |                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Enable                  | Enables saving the system logs to disk.                                                                                                                                                                                                                                                                                                                                                                                   |
| File Name               | Path and filename where the system log file is stored on the disk. The default is /local1/syslog.txt.                                                                                                                                                                                                                                                                                                                     |
| Priority                | Severity level of the message that should be sent to the specified remote syslog host.                                                                                                                                                                                                                                                                                                                                    |
| Recycle                 | The maximum size of the system log file before it is recycled. The default is 10000000 bytes.                                                                                                                                                                                                                                                                                                                             |
| <b>Host Settings</b>    |                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Enable                  | Enables sending the system log file to a host. You can configure up to four hosts.                                                                                                                                                                                                                                                                                                                                        |
| Hostname                | A hostname or IP address of a remote syslog host.                                                                                                                                                                                                                                                                                                                                                                         |
| Priority                | Severity level of the message that should be sent to the specified remote syslog host.                                                                                                                                                                                                                                                                                                                                    |
| Port                    | The destination port on the remote host. The default is 514.                                                                                                                                                                                                                                                                                                                                                              |
| Rate Limit              | The message rate per second. To limit bandwidth and other resource consumption, messages can be rate limited. If this limit is exceeded, the remote host drops the messages. There is no default rate limit, and by default all system log messages are sent to all syslog hosts.                                                                                                                                         |

**Step 6** Click **Submit** to save the settings.

## Multiple Hosts for System Logging

Each syslog host can receive different priority levels of syslog messages. Therefore, you can configure different syslog hosts with a different syslog message priority code to enable the device to send varying levels of syslog messages to the four external syslog hosts.

However, if you want to achieve syslog host redundancy or failover to a different syslog host, you must configure multiple syslog hosts on the device and assign the same priority code to each configured syslog host.

## Enabling the Kernel Debugger for Troubleshooting

The Kernel Debugger troubleshooting page allows you to enable or disable access to the kernel debugger. Once enabled, the kernel debugger is automatically activated when kernel problems occur.



### Note

The “hardware watchdog” is enabled by default and automatically reboots a device that has stopped responding for over ten minutes. Enabling the kernel debugger disables the “hardware watchdog.”

If the device runs out of memory and kernel debugger (KDB) is enabled, the KDB is activated and dump information. If the KDB is disabled and the device runs out of memory, the syslog reports only dump information and reboots the device.

To enable the kernel debugger:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Troubleshooting > Kernel Debugger**. The Kernel Debugger window appears.
  - Step 5** To enable the kernel debugger, check the **Enable** check box, and click **Submit**.
    - To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.
    - To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

For information about monitoring the SEs, see the [“Device Monitoring” section on page 10-9](#).

## Configuring Service Router Settings

The keep-alive interval is used by the SE to send keep-alive messages to the SR.

To configure the keep-alive interval the SE uses for messages to this SR:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options.
  - Step 4** Choose **General Settings > Service Routing Settings**. The Service Routing Settings page is displayed.
  - Step 5** In the **Keepalive-Interval** field, enter the number of seconds the messages from the SR should be kept alive on this SE. The range is from 1 to 120. The default is 2.
  - Step 6** Click **Submit** to save the settings.
    - To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

- To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Where to Go Next

Proceed to [Chapter 6, “Configuring the Service Router.”](#)

**Tip**

---

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Configuration Guide on Cisco.com.

---





## CHAPTER 6

# Configuring the Service Router

The following sections describe how to configure a Service Router (SR):

- [Activating a Service Router, page 6-1](#)
- [Configuring Application Control, page 6-3](#)
- [Configuring Last-Resort Routing, page 6-4](#)
- [Configuring Transaction Logs for the Service Router, page 6-7](#)
- [Where to Go Next, page 6-9](#)



### Tip

For information on configuring the general settings, except last-resort routing and transaction logging, see the [“General Settings” section on page 5-64](#).

## Activating a Service Router

Activating an SR can be done through the Devices home page initially, or through the Device Activation page.

To activate an SR from the Device Activation page:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options, and choose **Device Activation**. The Device Activation page is displayed.
- Step 4** Enter the settings as appropriate. See [Table 6-1](#) for a description of the fields.

**Table 6-1**      **Service Router Activation Fields**

| Field    | Description                                                                 |
|----------|-----------------------------------------------------------------------------|
| Name     | Name of the device.                                                         |
| Location | The Location drop-down list lists all the location configured for the ECDS. |

**Table 6-1**      **Service Router Activation Fields (continued)**

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Activate           | <p>To activate or deactivate the device, check or uncheck the <b>Activate</b> check box. Alternatively, you can click the <b>Deactivate Device</b> icon in the task bar.</p> <p>When you uncheck the <b>Activate</b> check box and click <b>Submit</b>, the <b>Replaceable</b> check box is displayed. Check the <b>Replaceable</b> check box when you need to replace the device or recover lost registration information. For more information, see the <a href="#">“Recovering ECDS Network Device Registration Information”</a> section on page 11-18.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server Offload     | <p>To offload this device for maintenance or a software upgrade, check the <b>Server Offload</b> check box. When checked, the Service Router stops processing client requests.</p> <p>When the SR is marked as inactive or is marked with server offload on the CDSM it stops responding to DNS queries. Instead, the SR sends a SERVFAIL error as the DNS response, and for RTSP/HTTP requests, the SR sends a 503 Service Unavailable message.</p> <p>To monitor the current activity on an SR during the Server Offload state, use the <b>show interface</b> command. If the packets received or packets sent is increasing then the SR is processing client requests.</p> <p><b>Note</b> We recommend separating the management traffic from the client request traffic by using the port channel configuration.</p> <ul style="list-style-type: none"> <li>• If management and client request traffic are separated, the <b>show interface</b> command for the client request port channel displays information on active sessions.</li> <li>• If management and streaming traffic are not separated, the <b>show interface</b> command shows very low traffic; the packets received and packets sent are lower than a client request session.</li> </ul> <p>Once the SR has finished processing client requests, you can perform maintenance or upgrade the software on the device. For information about upgrading the software, see the <a href="#">“Upgrading Software”</a> section on page 11-1.</p> <p>The Status field on the Device Activation page and the Devices Table page displays “offloading” when <b>Server Offload</b> is checked.</p> <p>Once the software upgrade or maintenance is complete, you need to uncheck the <b>Server Offload</b> check box so that the device can again participate in the system.</p> |
| Work Type          | <p>From the <b>Work Type</b> drop-down list, choose <b>Service Router only</b>. The <b>SR &amp; Proximity Engine</b> option is not supported.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Coverage Zone File | <p>To have a local Coverage Zone file overwrite the ECDS network-wide Coverage Zone file, choose a file from the <b>Coverage Zone</b> drop-down list. See the <a href="#">“Coverage Zone File Registration”</a> section on page 9-11 for information about creating and registering a Coverage Zone file. Otherwise, choose <b>None</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 6-1 Service Router Activation Fields (continued)**

| Field                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use SR's primary IP address      | <p>Enables the CDSM to use the IP address on the primary interface of the SR for management communications.</p> <p><b>Note</b> If the <b>Use SR's primary IP Address for Management Communication</b> check box is checked and the Management Communication Address and Port are configured, the CDSM uses the SR's primary IP address for communication.</p> <p><b>Note</b> Do not check the <b>Use SR's primary IP Address for Management Communication</b> check box if you want to separate management and streaming traffic. Instead, use the Management Communication Address and Port fields to specify where management traffic should be sent.</p> |
| Management Communication Address | <p>Manually configures a management IP address for the CDSM to communicate with the SR.</p> <p>Manual configuration of the management IP address and port are used when using port channel configuration to separate management and streaming traffic. For more information about port channel configuration see the <a href="#">“Configuring Port Channel and Load Balancing Settings” section on page 5-83</a>.</p>                                                                                                                                                                                                                                       |
| Management Communication Port    | Port number to enable communication between the CDSM and the SR.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Comments                         | Information about the settings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Step 5** Click **Submit** to save the settings.

## Configuring Application Control

The Application Control pages allow you to enable Flash Media Streaming, to enable HTTP proxy on an SR, and to enable HTTP 302 redirection for Windows Media Technology files with an .asx extension.

To configure the application control for the SR:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the SR you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options, and choose **Application Control**.
- Step 4** To enable Flash Media Streaming on the SR, choose **Flash Media Streaming > General Settings**. The Flash Media Streaming Settings page is displayed.
  - a. Check the **Enable Flash Media Streaming** check box.
  - b. Click **Submit**.
 

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

- Step 5** To enable service monitoring for Flash Media Streaming on the SR, choose **Flash Media Streaming > Service Monitoring**. The Service Monitoring Settings page is displayed.
- Check the **Enable Service Monitoring** check box.
  - Click **Submit**.  
To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.  
To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- Step 6** To enable HTTP proxy on the SR:
- Choose **Web > HTTP > HTTP Connections**. The HTTP Connections Settings page is displayed.
  - Check the **Enable Incoming Proxy** check box.
  - Enter the port numbers that receive HTTP in the associated field.  
Separate each port number by a space. The default is port 80.
  - Click **Submit** to save the settings.  
To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.  
To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- Step 7** To enable the HTTP 302 redirection for Windows Media Technology files with an .asx extension:
- Choose **Web > HTTP > HTTP Redirect**. The HTTP Redirect Settings page is displayed.
  - Check the **Enable HTTP 302 for .asx File** check box.
  - Click **Submit**.  
To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.  
To remove the settings from the device, click the **Remove Settings** icon in the task bar.
- 

## Configuring Last-Resort Routing

Last-resort routing is useful when all Service Engines have exceeded their thresholds or all Service Engines in the domain are offline, or the client is unknown. If last-resort routing is configured, the Service Router redirects requests to a configurable alternate domain when all Service Engines serving a client network region are unavailable, or the client is unknown. A client is considered unknown if the client's IP address is not part of a subnet range listed in the Coverage Zone file or part of a defined geographical area listed in the Coverage Zone file.

See the following sections:

- [Creating a New Service, page 6-5](#)
- [Error File Name Examples, page 6-6](#)
- [Creating ASX Error Message Files for Windows Media Live Programs, page 6-7](#)



### Note

If the last-resort domain is not configured and the Service Engine thresholds are exceeded, known client requests are redirected to the origin server and unknown clients will either receive an error URL (if the Error Domain and Error Filename fields are configured), or a 404 “not found” message.

Unknown clients are only redirected to the alternate domain (last-resort domain) when the **Allow Redirect All Client Request** check box is checked or the equivalent **service-router last-resort domain <RFQDN> allow all** command is entered.



**Tip**

For more information, see the “[Last-Resort Routing](#)” section on page 1-24.

For information about configuring all general settings, except last-resort routing, see the “[General Settings](#)” section on page 5-64.

## Creating a New Service

To configure last-resort routing:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the SR you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.
- Step 4** Choose **General Settings > Last Resort**. The Last Resort Table page is displayed.  
The table is sortable by clicking the column headings.
- Step 5** Click the **Create New** icon.  
Click the **Edit** icon next to the domain name to edit a table entry.
- Step 6** Enter the settings as appropriate. See [Table 6-2](#) for a description of the fields.

**Table 6-2 Service Router Last Resort Fields**

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain Name                       | The Service Routing Domain Name (SRDN) (for example, srfqdn.cisco.com).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Allow Redirect All Client Request | <p>Check the <b>Allow Redirect All Client Request</b> check box to redirect all unknown clients to the alternate domain or content origin.</p> <p>If the <b>Allow Redirect All Client Request</b> check box is not checked, unknown clients (clients’ subnets are not included in the Coverage Zone file) receive a 404 message if the error URL is not configured. If the error URL is configured, client requests are redirected to the Error URL.</p> <p>If the <b>Allow Redirect All Client Request</b> check box is checked, unknown client requests are redirected to the alternate domain; otherwise, they are redirected to the origin server.</p> |
| Alternate Domain Name             | <p>The domain (for example, www.cisco.com) used to route requests to when the SEs are unavailable, or the client is unknown. A client is considered unknown if the client’s IP address is not part of a subnet range listed in the Coverage Zone file.</p> <p>If an Alternate Domain Name is not specified, requests for the domain entered in the Domain Name are routed to the origin server.</p> <p>The Alternate Domain Name could be a domain outside the ECDS. It could be a third-party CDN or external server. No DNS lookup is performed by the SR to check the liveness of this domain.</p>                                                      |

**Table 6-2**      **Service Router Last Resort Fields (continued)**

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Error Domain Name | <p>To redirect the request to an error URL for any unknown clients or when all SEs in the delivery service are unavailable, enter the domain name of the URL.</p> <p>The Error Domain Name could be a domain outside the ECDS. It could be a third-party CDN or external server. No DNS lookup is performed by the SR to check the liveness of this domain.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Error File Name   | <p>The filename of the error URL (for example, error.html or error/errorfile.flv).</p> <p>The error URL is made using the Error Domain Name plus the Error File Name. The Error File Name could be a filename with an extension (for example, error.html or errorfile.flv), or a directory and filename (for example, error/errorfile.flv or reroute/reroute.avi), or a filename without an extension. If no extension is specified, the extension is determined by the protocol used in the request.</p> <p>If a filename has a specific extension, and the request comes from a protocol that does not support the configured extension, the filename extension is automatically changed to an extension that is supported by the protocol.</p> <p><b>Note</b> For Flash Media Streaming, an external FMS server must exist that hosts an application for error handling. The SR redirects Flash Media Streaming requests to an application on the external FMS server. An example of a Flash Media Streaming error URL is <code>rtpm://errordomain.com/&lt;application&gt;</code>, where the application name is any application hosted on that server. The Error File Name, in the case of Flash Media Streaming, is the name of the application.</p> <p>See the <a href="#">“Error File Name Examples”</a> section on page 6-6.</p> |

**Step 7** Click **Submit** to save the settings. The entry is added to the Last Resort Table.

To delete a last-resort configuration, click the **Edit** icon for the configuration, then click the **Delete** icon in the task bar.

## Error File Name Examples

- Domain Name—wmt.cdsordis.com
- Error Domain Name—ssftorig.ssft.com
- Error File Name—testMessage

This configuration states that for any request where the domain name is wmt.cdsordis.com, if the client IP address is not included in the Coverage Zone file (or the client is not part of a defined geographical area if location-based routing is enabled) or there are no available SEs assigned to the delivery service, redirect the request to ssftorig.ssft.com/testMessage.<original\_extension>.

For example, if the client request was `http://wmt.cdsordis.com/vod/video.wmv` and the service rule conditions were met, the client would receive a 302 redirect to `http://ssftorig.ssft.com/testMessage.wmv`.

If you want the Error File Name to reside in a different directory, you can configure that as well. If the error message file was located in the “vod” directory, then the Error File Name would be configured as `vod/testMessage`.

## Creating ASX Error Message Files for Windows Media Live Programs



### Note

When redirecting a client request for live Windows Media Streaming programs, the error message must have the same format because live programs deliver an ASX file to the client. If you try to use an HTML or JPEG instead of an ASX file, the redirect will not work because the Windows Media player is trying to parse the ASX file.

To satisfy the requirements of the Windows Media player, create an ASX file for the error message file and put the URL to the error message file inside the ASX file. For example, below is a simple ASX file.

```
<ASX VERSION="3.0"> <Entry>

<REF HREF="http://<IP-Address-of-Server/path/filename"/>

</Entry> </ASX>
```

If you wanted the error file to be a GIF file on server 3.1.1.1 called testMessage.gif under the directory vod then this file would look like:

```
<ASX VERSION="3.0"> <Entry>

<REF HREF="http://3.1.1.1/vod-ecds/testMessage.gif"/>

</Entry> </ASX>
```

There are other ways to use an ASX file to display information. Below is an example of an approach to have the Windows Media player display an HTML web page with PARM HTMLView.

```
<ASX version="3.0"> <PARAM name="HTMLView"
value="http://111.254.21.99/playlist/error.htm"/> <REPEAT> <ENTRY>

<REF href="http://3.1.1.1/vod-ecds/testMessage.gif"/>

</ENTRY> </REPEAT> </ASX>
```

There are many ways to format and structure ASX files to display whatever error message you want, in whatever format you want.

## Configuring Transaction Logs for the Service Router

Transaction logs allow administrators to view the traffic that has passed through the SR. The fields in the transaction log are the client's IP address, the date and time when a request was made, the URL that was requested, the SE selected to serve the content, the protocol, and the status of the redirect. The SR transaction log file uses the W3C Common Log file format. For more information about transaction logs and their formats, see the [“Service Router Transaction Log Fields” section on page 10-63](#).

To enable transaction logging for the SR:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options.

- Step 4** Choose **General Settings > Notification and Tracking > Transaction Logging**. The Transaction Log Settings page is displayed.
- Step 5** Enter the settings as appropriate. See [Table 6-3](#) for a description of the fields.

**Table 6-3 Transaction Log Settings Fields**

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General Settings</b>            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Transaction Log Enable             | Enables transaction logging.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Compress Files before Export       | When this check box is checked, archived log files are compressed into gzip format before being exported to external FTP servers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Archive Settings</b>            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Max size of Archive File           | Maximum size (in kilobytes) of the archive file to be maintained on the local disk. The range is from 1,000 to 2,000,000. The default is 2,000,000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Max number of files to be archived | Maximum number of files to be maintained on the local disk. The range is from 1 to 1000. The default is 50.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Archive occurs                     | How often the working log is archived and the data is cleared from the working log. Choose one of the following: <ul style="list-style-type: none"> <li>Choose <b>every</b> to archive every so many seconds, and enter the number of seconds for the interval. The range is from 120 to 604800.</li> <li>Choose <b>every hour</b> to archive using intervals of one hour or less, and choose one of the following: <ul style="list-style-type: none"> <li><b>at</b>—Specifies the minute in which each hourly archive occurs</li> <li><b>every</b>—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30)</li> </ul> </li> <li>Choose <b>every day</b> to archive using intervals of one day or less, and choose one of the following: <ul style="list-style-type: none"> <li><b>at</b>—Specifies the hour in which each daily archive occurs</li> <li><b>every</b>—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24)</li> </ul> </li> <li>Choose <b>every week on</b> to archive at intervals of one or more times a week, choose the days of the week, and choose what time each day.</li> </ul> |
| <b>Export Settings</b>             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Enable Export                      | Enables exporting of the transaction log to an FTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



**Table 6-3 Transaction Log Settings Fields (continued)**

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Export occurs     | <p>How often the working log is sent to the FTP server and the data is cleared from the working log. Choose one of the following:</p> <ul style="list-style-type: none"> <li>Choose <b>every</b> to export every so many minutes, and enter the number of minutes for the interval. The range is from 1 to 100800.</li> <li>Choose <b>every hour</b> to export using intervals of one hour or less, and choose one of the following: <ul style="list-style-type: none"> <li><b>at</b>—Specifies the minute in which each hourly export occurs</li> <li><b>every</b>—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30)</li> </ul> </li> <li>Choose <b>every day</b> to export using intervals of one day or less, and choose one of the following: <ul style="list-style-type: none"> <li><b>at</b>—Specifies the hour in which each daily export occurs</li> <li><b>every</b>—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24)</li> </ul> </li> <li>Choose <b>every week on</b> to export using intervals of one or more times a week, choose the days of the week, and what time each day.</li> </ul> |
| FTP Export Server | IP address or hostname of the FTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Name              | Name of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Password          | Password for the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Confirm Password  | Confirms the password for the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Directory         | Name of the directory used to store the transaction logs on the FTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SFTP              | Check the <b>SFTP</b> check box, if you are using an SFTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Step 6** Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

## Where to Go Next

Proceed to [Chapter 7, “Configuring WCCP.”](#)



### Tip

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Configuration Guide on Cisco.com.





# CHAPTER 7

## Configuring WCCP

---

The following sections describe the Web Cache Communication Protocol (WCCP) feature for Cisco Enterprise Content Delivery System (ECDS):

- [Configuring WCCP General Settings, page 7-1](#)
- [Configuring WCCP Services, page 7-3](#)
- [Managing WCCP Router Lists, page 7-12](#)
- [Managing WCCP Port Lists, page 7-15](#)
- [Configuring WCCP Transparent Routing Bypass Settings, page 7-18](#)
- [Creating WCCP Bypass List Entries, page 7-19](#)
- [Configuring HTTP IP Spoofing with WCCP, page 7-19](#)
- [Basic WCCP CLI Configuration Examples, page 7-21](#)
- [Where to Go Next, page 7-30](#)

## Configuring WCCP General Settings

To use WCCP, the Service Engine must be properly configured. To use a WCCP-enabled router, an IP address must be configured on the router interface that is connected to the Internet, and this interface must be visible to the Service Engine on the network.

To configure WCCP general settings:

- 
- Step 1** Log into the ECDS administration GUI.
  - Step 2** Choose **Devices > Devices**. A list of devices is displayed.
  - Step 3** Click the **Edit** icon next to the Service Engine for which you want to configure WCCP service settings. The Device Home for Service Engine window displays.
  - Step 4** Choose **Request Routing > WCCP > General Settings**. The WCCP Configuration Settings window displays ([Figure 7-1](#)). [Table 7-1](#) describes the fields and provides CLI information.
  - Step 5** Enable WCCP Version 2 by choosing **2** from the WCCP Version menu. Only WCCP Version 2 is supported with Cisco ECDS.

Figure 7-1 Configuring WCCP General Settings

The screenshot shows the Cisco Enterprise Content Delivery System Manager interface. The top navigation bar includes 'Devices', 'Services', and 'System'. The left sidebar shows a tree view with 'WCCP' expanded under 'Request Routing'. The main content area displays 'WCCP Configuration Settings for Service Engine, fai-mde3700'. The settings are as follows:

| Parameter                | Value                               |
|--------------------------|-------------------------------------|
| WCCP Version:            | 2                                   |
| Enable Flow Redirection: | <input checked="" type="checkbox"/> |
| Slow Start:              | <input checked="" type="checkbox"/> |
| Shutdown Delay:          | 120 (0-86400) seconds               |

Current settings: None (Using Factory Defaults)

Note: \* - Required Field

Buttons: Submit, Cancel

Table 7-1 WCCP General Settings Commands

| GUI Parameter           | Function                                                                                                                          | CLI Command                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| WCCP Version            | Enables WCCP Version 2. To disable WCCP, use the <b>no</b> form of this command.                                                  | <b>wccp version 2</b>                           |
| Enable Flow Redirection | Keeps the TCP flow intact.                                                                                                        | <b>wccp flow-redirect enable</b>                |
| Slow Start              | Enables slow start caching service on a Service Engine. To disable slow start capability, use the <b>no</b> form of this command. | <b>wccp slow-start enable</b>                   |
| Shutdown Delay          | Maximum amount of time (in seconds) the Service Engine waits to perform a clean shutdown of WCCP.                                 | <b>wccp shutdown max-wait</b><br><i>seconds</i> |

**Step 6** To keep the TCP flow intact, and to avoid overwhelming Service Engines when they come up or are reassigned new traffic, check the **Enable Flow Redirection** check box. This feature also has a slow start mechanism which enables a Service Engine to manage an amount of data that is appropriate for its capacity (see [Step 7](#)).

Use the **wccp flow-redirect enable** command.

**Step 7** To enable the slow start capability on the Service Engine, check the **Slow Start** check box. For more information about the WCCP Slow Start feature, see the “[Slow Start](#)” section on page 2-21.

Use the **wccp slow-start enable** command.

**Step 8** In the Shutdown Delay field, specify the maximum amount of time (in seconds) the Service Engine waits to perform a clean shutdown of WCCP. For more information about WCCP shutdown delay, see the “Graceful (Clean) Shutdown” section on page 2-20.

Use the **wccp shutdown max-wait** command.

**Step 9** Click **Submit** to save your settings.

## Configuring WCCP Services

See the following sections:

- [Configuring WCCP Service Settings, page 7-3](#)
- [Managing WCCP Service Masks, page 7-9](#)
- [Managing WCCP Router Lists, page 7-12](#)
- [Managing WCCP Port Lists, page 7-15](#)

## Configuring WCCP Service Settings

To configure WCCP service settings for the Service Engine:

**Step 1** Choose **Request Routing > WCCP > Services**. The WCCP Service Settings for Service Engine window appears (Figure 7-2).



**Note**

The Service Engine settings or its associated device group settings will be applied to this window depending on the choice that you have made in the WCCP General Settings window.

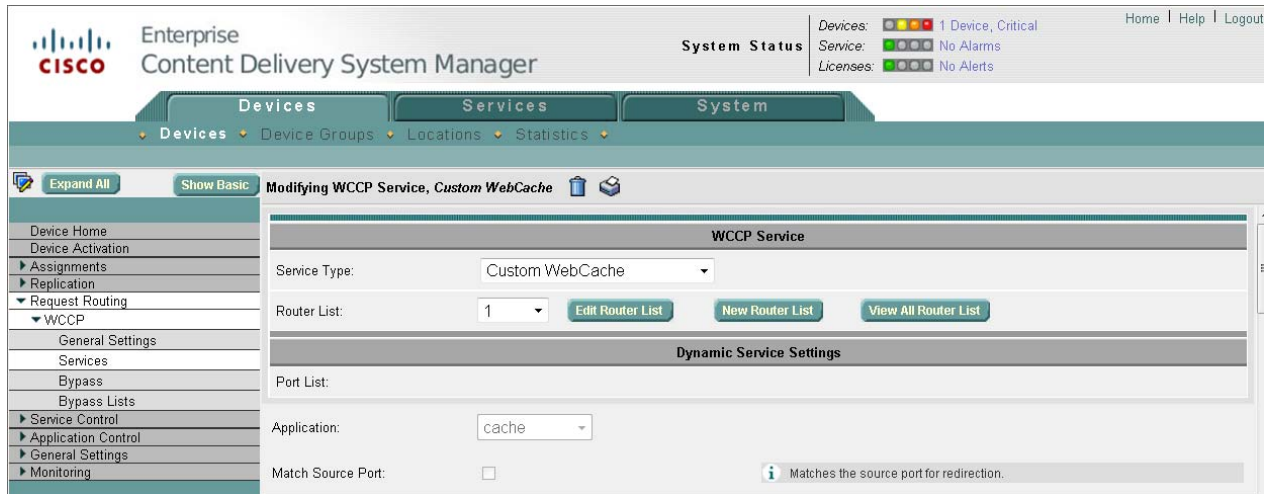
**Figure 7-2 WCCP Service Settings**

The screenshot displays the Cisco Enterprise Content Delivery System Manager interface. The top navigation bar includes 'Devices', 'Services', and 'System'. The 'Services' tab is active, showing 'WCCP Service Settings for Service Engine, r1se1'. The left sidebar contains a tree view with 'Request Routing' expanded, showing 'WCCP' and 'General Settings'. The main content area shows a table with columns 'Service' and 'Router List'. The table lists the following services and their corresponding router list values:

| Service             | Router List |
|---------------------|-------------|
| HTTPS               | 1           |
| RTMP                | 1           |
| RTSP                | 1           |
| WebCache            | 1           |
| Windows Media       | 1           |
| Windows Media RTSPU | 1           |

- Step 2** To edit an existing service, click a service icon in the Service section. The Modifying page for that service is displayed. [Figure 7-3](#) shows an example of the Custom WebCache service page.

**Figure 7-3** Modifying WCCP Service Window



- Step 3** Manage the following services from the WCCP Service Settings for Service Engine page:

- [Creating New WCCP Service, page 7-4](#)
- [Configuring WCCP Services, page 7-5](#)
- [Configuring Dynamic Service Settings, page 7-6](#)
- [Configuring Load Balancing Hash, page 7-6](#)
- [Configuring Other Settings, page 7-7](#)
- See also [Enabling WCCP on the Router](#).

## Creating New WCCP Service

To create new WCCP service:

- Step 1** Click the **Create New WCCP Service Setting** icon in the taskbar. The Creating New WCCP Service window appears.
- Step 2** Configure a maximum of seventeen services. If seventeen services have already been defined, the Create New WCCP Service Settings icon is not visible in the taskbar.



**Note** Settings for a particular WCCP service can be configured only after the WCCP service has been associated with a router list. See the [“Creating WCCP Router Lists” section on page 7-12](#).

- Step 3** Proceed to [Configuring WCCP Services](#).

## Configuring WCCP Services

In the WCCP Service section:

- Step 1** Choose the type of WCCP service from the Service Type drop-down list. (See [Table 7-2](#) for a description of the service types.)

**Table 7-2 WCCP Service Types**

| Service Type           | Service Group Number | Description of Services                                                                                                                                                                                               | CLI Command                  |
|------------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| WebCache               | 0                    | Enables web cache service with WCCP Version 2. With web cache service, the router balances the traffic load within a Service Engine cluster based on the destination IP address (for example, web server IP address). | <b>wccp web-cache</b>        |
| HTTPS                  | 70                   | Enables WCCP flow redirection to a Service Engine configured as an HTTPS server.                                                                                                                                      | <b>wccp https</b>            |
| RTSP                   | 80                   | Configures WCCP Version 2 Real-Time Streaming Protocol (RTSP) transparent interception.                                                                                                                               | <b>wccp rtsp</b>             |
| Windows Media          | 81-82                | Enables WCCP Version 2 Windows Media caching service.                                                                                                                                                                 | <b>wccp wmt</b>              |
| Windows Media RTSPU    | 83                   | Enables Windows Media RTSPU (port 5005) transparent interception.                                                                                                                                                     | <b>wccp wmt-rtspu</b>        |
| RTMP                   | 84                   | Managed domains.                                                                                                                                                                                                      | <b>wccp rtmp</b>             |
| Custom WebCache        | 98                   | Enables the Service Engine to accept redirected HTTP traffic on a port other than 80.                                                                                                                                 | <b>wccp custom-web-cache</b> |
| Dynamic Service Number | 90-97                | Enables up to eight dynamic WCCP redirection services on the Service Engine.                                                                                                                                          | <b>wccp service-number</b>   |

- Step 2** Associate a router list with the WCCP service by choosing one from the Router List drop-down list.



**Tip** Only configured router lists are displayed in the drop-down list.

See the following sections for more information about router lists:

- [Creating WCCP Router Lists, page 7-12](#)
- [Modifying WCCP Router Lists, page 7-13](#)
- [Viewing WCCP Router Lists, page 7-14](#)

- Step 3** Proceed to [Configuring Dynamic Service Settings, page 7-6](#)

## Configuring Dynamic Service Settings

In the Dynamic Service Settings section:

- Step 1** To associate ports with specific WCCP Version 2 dynamic services, choose the port list number from the **Port List** drop-down menu. [Figure 7-4](#) shows the Dynamic Service Settings section of the Creating New WCCP Service page.

**Figure 7-4** *Dynamic Service Settings*

All configured port lists are displayed here. You can only associate ports with user-configurable web cache services 90–97. For all other services, the Port List drop-down menu is disabled.



**Tip** To configure a port list for WCCP Version 2 dynamic services or if no port list already exists, see the [“Configuring WCCP Port Lists”](#) section on page 7-15.

- Step 2** From the Application drop-down list, choose the application running on the Service Engine to which intercepted traffic must be redirected. [Table 7-3](#) describes the available options.

**Table 7-3** *Application Redirect Options*

| Option      | Description                                                                         |
|-------------|-------------------------------------------------------------------------------------|
| cache       | Redirects traffic to the caching application running on the Service Engine.         |
| https-cache | Redirects traffic to the HTTPS caching application running on the Service Engine.   |
| streaming   | Redirects traffic to the streaming media application running on the Service Engine. |

- Step 3** To match the source port for traffic redirection, select the **Match Source Port** check box.

- Step 4** Proceed to [Configuring Load Balancing Hash](#).

## Configuring Load Balancing Hash

In the Load Balancing Hash section:

- Step 1** To define the destination IP address load-balancing hash, check the **Destination IP** check box. Use the `wccp web-cache router-list-num 1 hash-destination-ip` command. [Figure 7-5](#) shows the Load Balancing Hash section of the Creating New WCCP Service page.



**Figure 7-5 Load Balancing Hash Settings**

| Load Balancing Hash |                                     |              |                          |
|---------------------|-------------------------------------|--------------|--------------------------|
| Destination IP:     | <input checked="" type="checkbox"/> | Source IP:   | <input type="checkbox"/> |
| Destination Port:   | <input type="checkbox"/>            | Source Port: | <input type="checkbox"/> |

**Step 2** To define the source IP address load-balancing hash, select the **Source IP** check box. This method is the default hash assignment for HTTPS cache service.

Use the **wccp web-cache router-list-num 1 hash-source-ip** command.

**Step 3** To define destination port load-balancing hash, select the **Destination Port** check box.

Use the **wccp web-cache router-list-num 1 hash-destination-port** command.

**Step 4** To define the source port load-balancing hash, select the **Source Port** check box.

Use the **wccp web-cache router-list-num 1 hash-source-port** command.



**Tip** For most WCCP services, the destination IP is used for the default hashing target. For HTTPS service, the source IP is used for the default hashing target.

**Step 5** Proceed to [Configuring Other Settings](#).



**Tip** For command examples, see the [“Load Balancing Command Examples” section on page 7-22](#).

## Configuring Other Settings

In the Other Settings section:

**Step 1** To force WCCP to use the configured assignment method only, select the **Use Selected Assignment Method** check box. This setting can be configured only for HTTPS cache, custom web cache, web cache, and Windows Media services. When applied, both hash and mask assignment load balancing methods can be used.

[Figure 7-6](#) shows the Other Settings section of the Creating New WCCP Service page.

**Figure 7-6 Other Settings**

| Other Settings                    |                                           |                                                                    |
|-----------------------------------|-------------------------------------------|--------------------------------------------------------------------|
| Use Selected Assignment Method:   | <input type="checkbox"/>                  | Forces WCCP to strictly use only the configured assignment method. |
| Layer2 Redirection:               | <input type="checkbox"/>                  | Forwards packet by Layer 2 redirect.                               |
| Packet return by Layer 2 rewrite: | <input type="checkbox"/>                  | Packet return by Layer 2 rewrite.                                  |
| Password:                         | <input type="password"/>                  | Password used to authenticate.                                     |
| Confirm Password:                 | <input type="password"/>                  |                                                                    |
| Assignment Weight:                | <input type="text" value="0"/> (0-10000)  | Assignment Weight used for load balancing.                         |
| Port:                             | <input type="text" value="80"/> (1-65535) |                                                                    |
| Use Mask Assignment:              | <input type="checkbox"/>                  | Uses the mask method for Content Engine assignment.                |

**Step 2** To rewrite the packet Layer 2 MAC addresses to forward packets to the Service Engine, select the **Layer2 Redirection** check box.

Use the **wccp web-cache router-list-num 1 l2-redirect** command.

If negotiation fails using this method, negotiation uses the default GRE method instead.

**Step 3** To rewrite the packet Layer 2 MAC addresses to return packets to the switch, select the **Packet return by Layer 2** rewrite check box.

Use the **wccp web-cache router-list-num 1 l2-return** command.

If negotiation fails using this method, negotiation uses the default GRE method instead.

**Step 4** In the **Password** field, specify the password to be used for secure traffic between the Service Engines within a cluster and the router for a specified service. Be sure to enable all other Service Engines and routers within the cluster with the same password.

Use the **wccp web-cache router-list-num 1 password** command.



**Tip** Passwords must not exceed 8 characters in length.

**Step 5** Reenter the password in the **Confirm Password** field.

**Step 6** In the **Assignment Weight** field, specify the weight parameter that represents a percentage of the total load redirected to the Service Engine (for example, a Service Engine with a weight of 30 receives 30 percent of the total load). If the total of all weight parameters in a Service Engine cluster exceeds 100, the percentage load for each Service Engine is recalculated as the percentage that its weight parameter represents of the combined total.

Use the **wccp web-cache router-list-num 1 weight** command.

**Step 7** In the **Port** field, specify the port number other than port 80 that will accept redirected HTTP traffic (configurable only for custom web cache service).

**Step 8** To use the mask method for Service Engine assignment instead of the hash method, check the **Use Mask Assignment** check box. If negotiation fails, negotiation uses the hash method, which is the default.

Use the following commands:

- **wccp web-cache router-list-num 1 mask-assign**—If mask negotiation fails, negotiation uses the hash method, which is the default.

- **wccp web-cache router-list-num 1 mask-assign assign-method-strict**—Mask assignment only. Use **assign-method-strict** to establish WCCP service exclusively. If negotiation fails or the router does not support WCCP, no WCCP service is created. If **mask-assign** and **assign-method-strict** both appear in the command, the result will be either mask assignment or no WCCP service.
- **wccp web-cache router-list-num 1 assign-method-strict**—Hash assignment only. Use **assign-method-strict** to establish WCCP service exclusively. If negotiation fails, no WCCP service is created. If **assign-method-strict** is specified, and the WCCP router does not support hash assignment, then WCCP service will not be successfully configured. If only **assign-method-strict** appears in the command, the result will be hash assignment only or no WCCP service.

**Step 9** Click **Submit** to save the settings on the WCCP Service page.

- To create a new WCCP service mask, click the **Create Mask** button. For more information about creating service masks, see the [“Configuring WCCP Service Masks” section on page 7-9](#).
- To modify or delete a configured service mask, click the **Edit Mask** button. For more information about modifying service masks, see the [“Modifying WCCP Service Masks” section on page 7-10](#).
- To view all configured service masks, click the **View Masks Configured for All Services** button. For more information about viewing service masks, see the [“Viewing WCCP Service Masks” section on page 7-11](#).

## Managing WCCP Service Masks

Use the information in this section to manage WCCP service masks:

- [Configuring WCCP Service Masks, page 7-9](#)
- [Modifying WCCP Service Masks, page 7-10](#)
- [Viewing WCCP Service Masks, page 7-11](#)
- [Viewing WCCP Service Masks, page 7-11](#)

## Configuring WCCP Service Masks

Bit masks are specified as hexadecimal numbers. All the specified bit masks together cannot have more than 7 bits set. For example, a correct way of using three masks is 0xF (4 bits), 0x1 (1 bit), and 0x3 (2 bits) for a total of 7 bits. In this case, you cannot configure any additional mask other than 0x0. Otherwise, an error message is displayed.

An example of using four masks could be 0xA (2 bits), 0x7 (3 bits), 0x8 (1 bit), 0x1 (1 bit) for a total of 7 bits. You can configure up to 16 WCCP service masks.

To configure WCCP service masks on the Service Engine:

- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the network.
- Step 2** Click the **Edit** icon next to the Service Engine for which you want to configure WCCP service masks. The Device Home for Service Engine window appears.
- Step 3** To display the entire table of contents, click the **Show All** button above the Contents pane.
- Step 4** In the Contents pane, choose **Request Routing > WCCP > Services**. The WCCP Service Settings for Service Engine window appears.

- Step 5** Click the **Create New WCCP Service Setting** icon in the taskbar to configure router lists for a new service. The Creating New WCCP Service window appears.
- Step 6** Alternatively, click the **Edit WCCP Service Setting** icon next to an existing WCCP service for which you want to configure router lists. The Modifying WCCP Service window appears.
- Step 7** Under the WCCP Service section, choose a WCCP service from the Service Type drop-down list.
- Step 8** Under the Other Settings section, click the **Create Mask** button next to the Use Mask Assignment check box to configure a service mask and associate it with a WCCP Version 2 service. The Creating New WCCP Service Mask window appears.
- Step 9** Choose the type of WCCP service from the Service Type drop-down list. [Table 7-2](#) describes these service types.
- Step 10** In the Source IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet source IP address. The range is 0x00000000–0xFE000000. The default is 0x00000000.
- Step 11** In the Source Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFE00) used to match the packet source port number. The port mask range is 0x00–0xFE. The default is 0x0.
- Step 12** In the Destination IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet destination IP address. The range is 0x00000000–0xFE000000. The default is 0x00001741.
- Step 13** In the Destination Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFE00) used to match the packet destination port number. The port mask range is 0x00–0xFE. The default is 0x0.
- Step 14** To save the settings, click **Submit**. The Creating New WCCP Service window or the Modifying WCCP Service window appears, depending on the window from which you navigated.
- 

## Modifying WCCP Service Masks

To modify a WCCP service mask on the Service Engine:

- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the ECDS network.
- Step 2** Click the **Edit** icon next to the Service Engine for which you want to configure WCCP service masks. The Device Home for Service Engine window appears.
- Step 3** To display the entire table of contents, click the **Show All** button above the Contents pane.
- Step 4** In the Contents pane, choose **Request Routing > WCCP > Services**. The WCCP Service Settings for Service Engine window appears.
- Step 5** Click the **Create New WCCP Service Setting** icon in the taskbar to configure router lists for a new service. The Creating New WCCP Service window appears.
- Alternatively, click the **Edit WCCP Service Setting** icon next to an existing WCCP service for which you want to configure router lists. The Modifying WCCP Service window appears.
- Step 6** Under the WCCP Service section, choose a WCCP service from the Service Type drop-down list.
- Step 7** Under the Other Settings section, click the **Edit Mask** button next to the Use Mask Assignment check box to modify a service mask and associate it with a WCCP Version 2 service. The Modifying WCCP Service Mask window appears.

- Step 8** The Edit Mask button toggles with the Create Mask button if a service mask has already been configured for a WCCP service.
- Step 9** Choose the type of WCCP service from the Service Type drop-down list. See [Table 7-2](#) for a description of the service types.
- Step 10** In the Source IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet source IP address. The range is 0x00000000–0xFE000000. The default is 0x00000000.
- Step 11** In the Source Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFE00) used to match the packet source port number. The port mask range is 0x00–0xFE. The default is 0x0.
- Step 12** In the Destination IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet destination IP address. The range is 0x00000000–0xFE000000. The default is 0x00001741.
- Step 13** In the Destination Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFC00) used to match the packet destination port number. The port mask range is 0x0–0xFE. The default is 0x0.
- Step 14** To save the settings, click **Submit**. The Creating New WCCP Service window or the Modifying WCCP Service window appears depending on the window from which you navigated.
- 

## Viewing WCCP Service Masks

To view all masks configured for a WCCP service:

- Step 1** From the Creating New WCCP Service window or Modifying WCCP Service window, click the **View Masks Configured for All Services** button to view all configured service masks for WCCP services. The WCCP Service Mask Settings for Service Engine window appears. A list of all services for which masks have been configured to match the packet source IP address, source port number, destination IP address, or destination port number are displayed.
- Step 2** To return to the Creating New WCCP Service or Modifying WCCP Service window, click the **Back** (left arrow) icon in the taskbar.
- Step 3** To configure a new service mask, click the **Create New WCCP Service Mask Setting** icon in the taskbar. The Creating New WCCP Service Mask window appears.
- Alternatively, click the **Edit WCCP Service Mask Setting** icon next to an existing WCCP service mask for which you want to change the mask settings. The Modifying WCCP Service Mask window appears.
- 

## Deleting a WCCP Service Mask

To delete a service mask on the Service Engine:

- Step 1** From the WCCP Service Mask Settings for Service Engine window, click the **Edit WCCP Service Mask Setting** icon next to an existing WCCP service mask for which you want to change the mask settings. The Modifying WCCP Service Mask window appears.

- Step 2** Click the **Delete WCCP Service Mask** icon in the taskbar. The system displays a dialog box asking you to confirm whether you want to permanently delete the service mask configuration.
- Step 3** Click **OK** to confirm. The WCCP Service Mask Settings for Service Engine window appears.

## Managing WCCP Router Lists

Use the information in this section to manage router lists while configuring WCCP services in **Devices > Request Routing > WCCP > Services**. See [“Configuring WCCP Services”](#) section on page 7-5 for more information.

- [Creating WCCP Router Lists, page 7-12](#)
- [Modifying WCCP Router Lists, page 7-13](#)
- [Viewing WCCP Router Lists, page 7-14](#)

## Creating WCCP Router Lists

You can create up to 8 different router lists with up to 32 IP addresses per list for use with WCCP Version 2 services. A router list must contain at least one IP address.

To create WCCP router lists:

- Step 1** Choose **Request Routing > WCCP > Services**.
- Step 2** Click the **New Router List** button. The Creating New WCCP Router window appears ([Figure 7-7](#)).

**Figure 7-7** WCCP New Router List

The screenshot shows the Cisco Enterprise Content Delivery System Manager interface. The top navigation bar includes 'Home | Help | Logout' and 'System Status' with indicators for Devices (1 Device, Critical), Service (No Alarms), and Licenses (No Alerts). The main navigation pane on the left lists various configuration options, with 'Request Routing' and 'WCCP' expanded. The central pane displays the 'Creating new WCCP Router List' window. This window features a 'List Number' dropdown menu currently set to '2'. Below the dropdown is a text input field labeled 'Add Router' and two buttons: 'Add Router>>>' and '<<<Remove Router'. A note at the bottom of the window indicates that an asterisk (\*) denotes a required field.

- Step 3** In the Router IP Address field, specify the IP address of the router to be added to the list.



### Tip

You must enter at least one IP address and all IP addresses added must be unique within the router list.

**Step 4** To add an IP address to the list, click **Add Router**. This list represents the IP address of every router that will redirect traffic to this Service Engine for a particular service. If different routers will be used for different services, you must create more than one router list.

The window refreshes and the addresses are listed in numerical order. The order might not match the order in which IP addresses were entered. IP addresses will be displayed in red until settings are saved.

**Step 5** To save the router list or to save any edits you have made to the router IP addresses, click **Submit**. You will be returned to the WCCP Service window.

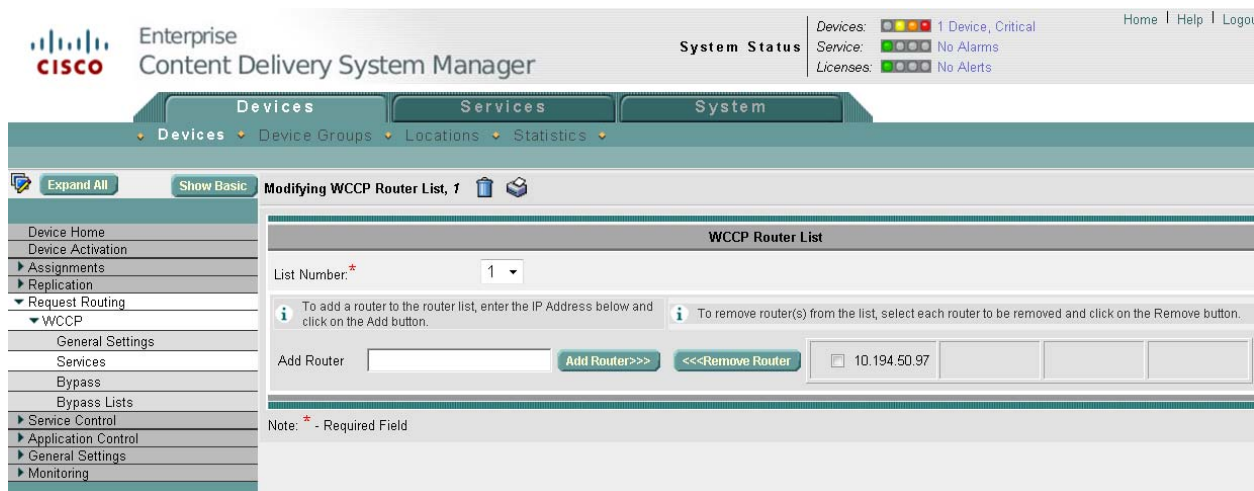
## Modifying WCCP Router Lists

To add or delete an IP address from a router list or to delete a router list:

**Step 1** From the Creating New WCCP Service window or Modifying WCCP Service window, choose the router list number from the List Number drop-down list.

**Step 2** Click the **Edit Router List** button. The Modifying WCCP Router List window appears (Figure 7-8).

**Figure 7-8** Modifying a WCCP Router List



**Step 3** To add a router to the router list, enter the router's IP address in the Router IP Address field, and click the **Add Router** button.

**Step 4** To remove a router from the router list, select the check box next to the router in the list and click the **Remove Router** button.

**Step 5** To modify the router IP address, click the **Edit IP Address** icon next to the IP address that you want to modify (Figure 7-9).



**Figure 7-9** Edit Router List

The screenshot shows the Cisco Enterprise Content Delivery System Manager interface. The top navigation bar includes 'Devices', 'Services', and 'System'. The left sidebar shows a tree view with 'Request Routing' expanded, showing 'WCCP' and 'General Settings'. The main content area is titled 'Modifying WCCP Service, WebCache'. It contains two sections: 'WCCP Service' and 'Dynamic Service Settings'. In the 'WCCP Service' section, 'Service Type' is set to 'WebCache' and 'Router List' is set to '1'. There are buttons for 'Edit Router List', 'New Router List', and 'View All Router List'. In the 'Dynamic Service Settings' section, 'Port List' is empty, 'Application' is set to 'cache', and 'Match Source Port' is unchecked with a note 'Matches the source port for redirection.'

- Step 6** The IP address will be displayed in the Router IP Address field. Once you have changed the IP address, click the **Edit** button to add the modified IP address to the list. The window refreshes itself, and the changed IP address will be displayed in purple until settings are saved.



**Tip** The **Edit** button next to the Router IP Address field is displayed as Add Router to allow you to add any new IP address to the list. The **Edit** button toggles with the **Add Router** button.

- Step 7** To save the settings, click **Submit**. The window refreshes itself, and the settings are saved.

- Step 8** To delete a router list, follow these steps:

- a. From the Modifying WCCP Router window, click the trash can icon (**Delete WCCP Router List**) in the taskbar. The system displays a dialog box asking you to confirm that you want to permanently delete the router list configuration.



**Note** When you delete a router list, the WCCP Version 2 services that have been configured to use this router list are also deleted. Make sure that the WCCP service is associated with a different router list, if required, before deleting the previously configured router list.

- b. Click **OK** to confirm. The selected router list and the services with which it is associated are deleted.

## Viewing WCCP Router Lists

To view all router lists configured for a WCCP Version 2 dynamic service:

- Step 1** To view all configured router lists for WCCP Version 2, click the **View All Router List** button from the Creating New WCCP Service window or the Modifying WCCP Service window. The WCCP Router List Configurations for Service Engine window appears.

The List Number column displays all configured router list numbers. The Router IP Addresses column displays a list of IP addresses that were added to the router list. From this window you can perform the following actions:



- Return to the previous window
- Edit an existing router list
- Create a new router list

- Step 2** To return to the Creating New WCCP Service window, click the **Back** arrow in the GUI taskbar.
- Step 3** To configure a new router list and add IP addresses from this window, click the **Create New WCCP Router List Configuration** icon in the taskbar. The Creating New WCCP Router List window appears.
- Step 4** To edit an existing router list, click the **Edit WCCP Router List Configuration** icon next to the router list that you want to modify. The Modifying WCCP Router window appears. You can add, update, or delete IP addresses.

**Tip**

For an example of the task bar icons, see the “[Task Bar](#)” section on page 3-9.

## Managing WCCP Port Lists

Use the information in this section to manage WCCP port lists:

- [Configuring WCCP Port Lists, page 7-15](#)
- [Modifying WCCP Port Lists, page 7-17](#)

## Configuring WCCP Port Lists

With eight custom services that use a maximum number of eight ports each, the maximum number of ports that can be specified for transparent redirection is 64.

The legacy custom web cache services (service number 98) can be configured with only one port. If only one legacy service is configured, the total maximum number of transparent redirection ports is 57. If both legacy services are configured, the maximum port total is 50.

All ports receiving HTTP that are configured as members of the same WCCP service share the following characteristics:

- They have the same hash or mask parameters as configured using the Creating New WCCP Service window.
- The service on individual ports cannot be stopped or started individually (WCCP Version 2 restriction).

With Service Engines in a farm, the following restrictions apply:

- All Service Engines that use the same WCCP service are required to configure the same list of ports and the same hash or mask parameters.
- A Service Engine that tries to join the farm with the same WCCP service using a different list of ports or different hash or mask parameters is rejected by the router.
- To change the port list for a particular WCCP service, WCCP service must be stopped on all involved Service Engines, and then all must be restarted with the new parameters.

### Procedure

To configure WCCP ports:

- Step 1** Choose **Devices > Devices**. The Devices window appears, listing all the device types configured in the network.
- Step 2** Click the **Edit** icon next to the Service Engine for which you want to configure WCCP port lists. The Device Home for Service Engine window appears.
- Step 3** To display the entire table of contents, click the **Show All** button above the Contents pane.
- Step 4** In the Contents pane, choose **Request Routing > WCCP > Services**. The WCCP Service Settings for Service Engine window appears.
- Step 5** Click the **Create New WCCP Service Setting** icon in the taskbar to configure router lists for a new service. The Creating New WCCP Service window appears.
- Step 6** Alternatively, click the **Edit WCCP Service Setting** icon next to an existing WCCP service for which you want to configure router lists. The Modifying WCCP Service window appears.
- Step 7** In the WCCP Service section, choose a WCCP dynamic redirection service from the Service Type drop-down list.
- Step 8** In the Dynamic Service Settings section, click the **New Port List** button to configure a port list number to associate ports for a WCCP Version 2 dynamic service (Figure 7-10).

**Figure 7-10**      **New Port List Button**

The screenshot shows the 'Dynamic Service Settings' window. It has three main sections: 'Port List:' with a 'New Port List' button; 'Application:' with a dropdown menu set to 'cache'; and 'Match Source Port:' with an unchecked checkbox and an information icon that says 'Matches the source port for redirection.'

The WCCP Port List Settings window appears (Figure 7-11).

**Figure 7-11**      **WCCP Port List Settings**

The screenshot shows the 'WCCP Port List Settings' window. It features a table with columns 'List Number' and 'Ports'. The 'Ports' column contains eight input fields for each list number. A 'Clear List' button is located at the end of each row. Below the table, there is a note: 'Note: \* - Required Field'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

| List Number | Ports                                                                                                                                                                   | Clear List               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| 1           | <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> | <input type="checkbox"/> |
| 2           | <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> | <input type="checkbox"/> |
| 3           | <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> | <input type="checkbox"/> |
| 4           | <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> | <input type="checkbox"/> |
| 5           | <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> | <input type="checkbox"/> |
| 6           | <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> | <input type="checkbox"/> |
| 7           | <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> | <input type="checkbox"/> |
| 8           | <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> | <input type="checkbox"/> |

Note: \* - Required Field

Submit Cancel

- Step 9** Under the Ports column and against a port list number, specify the port number to be added to the list. You can configure a maximum of 8 port numbers per list.
- Each port number added must be unique among all configured port lists. Otherwise, an error message is displayed on submit.
- For a port list, port numbers need not necessarily be entered in successive fields under the Ports column. Blank fields in between will be removed on submit and all added port numbers will be reordered and displayed in ascending order when you visit the window the next time.
- Step 10** Click **Submit** to save the settings. The Creating New WCCP Service window or Modifying WCCP Service window appears depending where you began.

## Modifying WCCP Port Lists

To modify a port list:

- Step 1** From the Creating New WCCP Service window or Modifying WCCP Service window, click the **Edit Port List** button to configure a port list for WCCP Version 2 dynamic services. The WCCP Port List Settings window appears.
- Step 2** To modify port numbers in the port list:
- Choose a port list number and edit any of the port numbers that you wish to change in the Ports column for that row.
  - Click **Submit** to save the settings. The Creating New WCCP Service window or Modifying WCCP Service window appears depending on the window from which you traversed.
- Step 3** To delete a port list:
- Check the **Clear List** check box next to the port list that you want to delete. All added port numbers will be removed from the port list.
  - Click **Submit** to save the settings. The Creating New WCCP Service window or Modifying WCCP Service window appears depending on the window from which you traversed.

To configure dynamic service on the port list, enter the following commands:

```
SE(config)# wccp port-list 1 5566
```

```
SE(config)# wccp service-number 91 router-list-num 1 port-list-num 1 application cache
```

This command example configures port 5566 on port list #1. At the same time dynamic service with service number 91 is created using preconfigured router-list-num 1 and using the cache application.

The following application types are supported:

|             |                                                                            |
|-------------|----------------------------------------------------------------------------|
| cache       | Redirects incoming traffic to port 80—Standard port for the HTTP server.   |
| https-cache | Redirects incoming traffic to port 443—Standard port for the HTTPS server. |
| streaming   | Redirects incoming traffic to port 554—Standard port for the RTSP server.  |

# Configuring WCCP Transparent Routing Bypass Settings

To configure WCCP bypass settings.

- Step 1** Choose **Request Routing > WCCP > Bypass**. The WCCP Bypass Settings window appears (Figure 7-12).

**Figure 7-12** Configuring WCCP Bypass Settings

| WCCP Bypass Settings                                      |                                     |
|-----------------------------------------------------------|-------------------------------------|
| Current applied settings from Service Engine, <i>SE</i>   |                                     |
| Bypass Enable:                                            | <input checked="" type="checkbox"/> |
| Load Bypass Enable:                                       | <input type="checkbox"/>            |
| Minimum interval between putting system to bypass mode: * | 4 (seconds) (4-600)                 |
| Time will last when system put into bypass mode: *        | 10 (minutes) (1-1440)               |
| Time interval for polling system back from bypass: *      | 2 (seconds) (2-600)                 |

- Step 2** To enable the Service Engine to bypass incoming requests from clients, select the **Bypass Enable** check box.



**Note** Some websites may not allow the Service Engine to connect directly on behalf of the client. To avoid a disruption of service when traffic is bypassed, the Service Engine can use authentication bypass to generate a dynamic access list for these client/server pairs. Authentication bypass triggers are also propagated upstream and downstream in an ECDS network environment.

- Step 3** Select the **Load Bypass Enable** check box to enable traffic bypass.  
Use the **bypass load enable** command.
- Step 4** In the **Minimum interval between putting system to bypass mode** field, enter a number of seconds between 4 and 600.  
Use the **bypass load time-interval** command.
- Step 5** In the **Time will last when system put into bypass mode** field, enter a number of minutes between 1 and 1440.
- Step 6** In the **Time interval for polling system back from bypass** field, enter a number of seconds between 2 and 600.
- Step 7** Click **Submit** to save the settings.

# Creating WCCP Bypass List Entries

To create WCCP bypass list entries:

- Step 1** Choose **Devices > Devices > Request Routing > WCCP > Bypass List**.
- Step 2** Click the **Create New WCCP Bypass List** icon. The Creating new WCCP Bypass List window appears (Figure 7-13).

**Figure 7-13** Configuring WCCP Bypass Lists

- Step 3** Enter the IP address for the client in the **Client Address** field.
- Step 4** Enter the IP address for the server in the **Server Address** field.
- Step 5** Check **Submit** to save the settings.

Use the following commands:

- To create a WCCP bypass list:  

```
bypass static {clientip [serverip | any-server] | any-client serverip}
```
- To bypass all except a specific server on a specific port:  

```
bypass static port 80 except-server 1.1.1.1
```

The system bypasses all the traffic to this port, except the traffic that has a destination IP on the configured list.



**Tip**

Each Service Engine can have up to 50 bypass list entries.

## Configuring HTTP IP Spoofing with WCCP



**Note**

You must configure WCCP before you can enable IP Spoofing. Disable the IP Spoofing feature by unchecking the Enable IP Spoofing check box in the ECDS GUI before configuring WCCP. See the [“Configuring WCCP General Settings” section on page 7-1](#) to enable WCCP.

When configured for IP spoofing, the Service Engine connects to the origin server using the client IP address instead of its own IP address.

IP Spoofing does not support the following:

- Non-HTTP protocols

- Multiple SEs

To configure IP Spoofing on WCCP-enabled system:

**Step 1** Choose **Devices > Devices > Application Control > Web > HTTP > HTTP Connections**.

**Step 2** Select the Enable IP Spoofing check box (Figure 7-14).

**Figure 7-14 IP Spoofing Check Box**

The screenshot shows the 'HTTP Connection Settings' for Service Engine **cc-sre910-1**. The 'Enable IP Spoofing' checkbox is checked. Other settings include 'Webengine Maximum Concurrent Connections' set to 2000, 'Enable Incoming Proxy' checked, and 'Enable Outgoing Proxy' checked. A table for 'Outgoing Proxy' shows Hostname 128.107.241.17 and Port 80.

| Outgoing Proxy |                | Acquirer Outgoing Proxy Authentication |          |          |                  |                  |                              |
|----------------|----------------|----------------------------------------|----------|----------|------------------|------------------|------------------------------|
|                | Hostname       | Port                                   | Username | Password | Confirm Password | NTLM User Domain | Disable basic authentication |
| 1 *            | 128.107.241.17 | 80                                     |          |          |                  |                  | <input type="checkbox"/>     |
| 2              |                |                                        |          |          |                  |                  | <input type="checkbox"/>     |

**Step 3** Click **Submit** to save the settings.

### IP Spoofing Commands

To configure IP Spoofing on a service group with a single router and a single Service Engine:

- Two WCCP services need to be configured on the Service Engine:

- Configure WCCP HTTP redirection.

```
wccp web-cache router-list-num [number]
```

- Configure WCCP dynamic service.

```
wccp service-number [number] router-list-num [number] port-list-num [number]
application cache match-source-port
```

- Two WCCP services need to be configured on the Router:

```
ip wccp web-cache
ip wccp [91]
```

- Two interface interception and redirection instances need to be configured on the Router:

- Enter the following on the interface to the Origin Server:

```
ip wccp web-cache redirect out
```

- Enter the following on the interface to Origin Server Clients:

```
ip wccp [91] redirect out
```



#### Note

To allow client request interception, the **ip wccp redirect out** command must be configured on those interfaces connected to the client and the WAN.

4. Enter the following on the interface to the Service Engine:

```
ip wccp redirect exclude in
```



**Note**

The router cannot identify requests coming from the Service Engine because the source IP address of the request is not that of Service Engine. To prevent these Service Engine requests from being returned to the Service Engine unresolved, the **ip wccp redirect exclude in** command must be applied to the WCCP-enabled router interface to which the Service Engine is connecting. The **ip wccp redirect exclude in** command prevents the WCCP-enabled router from intercepting any requests coming in on this interface.



**Caution**

If you are using IP Spoofing with multiple Service Engines, the traffic coming back from Origin Server must be redirected to the correct service engine or the flow will break. Because WCCP assignment cannot be controlled, IP Spoofing with multiple Service Engines is not recommended.

Use caution configuring multiple Service Engines to use HTTP proxy; the traffic destination IP will be different than expected.

## Basic WCCP CLI Configuration Examples

- [Enabling WCCP on the Router, page 7-21](#)
- [Configuring the Router List Example, page 7-22](#)
- [Configuring a Multiple Router/Multiple SE WCCP Service Example, page 7-22](#)
- [Configuring WCCP for Flash Media Streaming, page 7-22](#)
- [Load Balancing Command Examples, page 7-22](#)
- [Web Caching Command Examples, page 7-24](#)

## Enabling WCCP on the Router

To enable an interface to redirect web traffic to the Service Engine using WCCP Version 2, perform the following tasks beginning in global configuration mode on the router:

|               | Command                                                                             | Purpose                                                                                                                                                        |
|---------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>ip wccp enable</b>                                               | Enables the router to use WCCP.                                                                                                                                |
| <b>Step 2</b> | Router(config)# <b>ip wccp redirect-list</b><br>[ <i>number</i>   <i>acl-name</i> ] | Specifies the redirect access list. Only packets that match this access list are redirected. If you do not configure this command, all packets are redirected. |
| <b>Step 3</b> | Router(config)# <b>interface</b> <i>type number</i>                                 | Enters interface configuration mode.                                                                                                                           |
| <b>Step 4</b> | Router(config-if)# <b>ip web-cache redirect</b>                                     | Configures the interface connected to the Internet to redirect web traffic to the Service Engine.                                                              |

|        | Command                                                   | Purpose                                                                                                                                               |
|--------|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | Router(config-if)# <b>ip route-cache same-interface</b>   | (Optional) If the client and a Service Engine are located on the same network, configures the router to use the fast switching path on the interface. |
| Step 6 | Router(config-if)# <b>end</b>                             | Exits configuration mode.                                                                                                                             |
| Step 7 | Router(config)# <b>copy running-config startup-config</b> | Saves the configuration.                                                                                                                              |

## Configuring the Router List Example

Use the following commands for basic WCCP Version 2 router configuration:

```
Se(config)# wccp router-list N <ip-address-list>
Se(config)# wccp version 2
Se(config)# wccp port-list 1 8443
Se(config-if)# wccp web-cache router-list-num 1
Se(config-if)# wccp rtsp router-list-num 1
Se(config-if)# wccp wmt router-list-num 1
Se(config)# wccp https-cache router-list-num 1 hash-destination-ip
```

## Configuring a Multiple Router/Multiple SE WCCP Service Example

Use the following commands when configuring a multi-router, multi-Service Engine WCCP Service Group. In this example, IP addresses are being configured for SE 1 and 2, and routers 1 and 2:

```
SE1(config)# wccp router-list-num 1 R1-ip R2-ip
SE1(config)# wccp web-cache router-list-num 1
SE2(config)# wccp router-list-num 1 R1-ip R2-ip
SE2(config)# wccp web-cache router-list-num 1
SE(config)# wccp slow-start enable
SE(config)# no wccp slow-start enable
```

## Configuring WCCP for Flash Media Streaming

In order for the SE to actually handle the intercepted request (cache unmanaged vods/split unmanaged live streams) and not bypass the request directly to the origin, the following configuration must be entered on the desired SE:

```
SE (config)# bypass static port 1935 except-server <fms-orig>
SE (config)# flash-media-streaming application-virtual-path vod-ecds map live-ecds
```

## Load Balancing Command Examples

- [Hash Assignment Command Example, page 7-23](#)
- [Mask Assignment Command Example, page 7-23](#)
- [Weight Assignment Command Example, page 7-24](#)



## Hash Assignment Command Example

The following example configures RTSP service with the hash assignment method using the source IP:

```
SE1(config)# wccp rtsp router-list-num 1 hash-source-ip
```

Check your configuration using the following **show** command:

```
MF-3825#show ip wccp 80 detail
```

```
WCCP Client information:
 WCCP Client ID: 192.168.1.5
 Protocol Version: 2.0
 State: Usable
 Redirection: GRE
 Packet Return: GRE
 Assignment: HASH
 Initial Hash Info: 00000000000000000000000000000000
 00000000000000000000000000000000
 Assigned Hash Info: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
 00000000000000000000000000000000

 Hash Allotment: 128 (50.00%)
 Packets s/w Redirected: 44
 Connect Time: 06:11:51
 Bypassed Packets
 Process: 0
 CEF: 0
 Errors: 0

 WCCP Client ID: 192.168.1.54
 Protocol Version: 2.0
 State: Usable
 Redirection: GRE
 Packet Return: GRE
 Assignment: HASH
 Initial Hash Info: 00000000000000000000000000000000
 00000000000000000000000000000000
 Assigned Hash Info: 00000000000000000000000000000000
 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

 Hash Allotment: 128 (50.00%)
 Packets s/w Redirected: 0
 Connect Time: 00:46:50
 Bypassed Packets
 Process: 0
 CEF: 0
 Errors: 0
```

## Mask Assignment Command Example

Mask assignment is configured correctly by using the following command:

```
SE(config)# wccp web-cache mask src-ip-mask 0x1
SE(config)# wccp web-cache router-list-num 1 mask-assign
SE(config)# wccp web-cache mask src-ip-mask 0x1
SE(config)# wccp web-cache router-list-num 1 mask-assign
```

Check your configuration using the following **show** command:

```
router# show ip wccp web-cache detail
```

```
WCCP Client information:
 WCCP Client ID: 192.168.1.54
 Protocol Version: 2.0
```

```

State: Usable
Redirection: GRE
Packet Return: GRE
Packets Redirected: 0
Connect Time: 00:02:03
Assignment: MASK
Mask SrcAddr DstAddr SrcPort DstPort
---- -
0000: 0x00000001 0x00000000 0x0000 0x0000
Value SrcAddr DstAddr SrcPort DstPort SE-IP
---- -
0000: 0x00000000 0x00000000 0x0000 0x0000 0xC0A80136 (192.168.1.54)

WCCP Client ID: 192.168.1.5
Protocol Version: 2.0
State: Usable
Redirection: GRE
Packet Return: GRE
Packets Redirected: 0
Connect Time: 00:02:03
Assignment: MASK
Mask SrcAddr DstAddr SrcPort DstPort
---- -
0000: 0x00000001 0x00000000 0x0000 0x0000
Value SrcAddr DstAddr SrcPort DstPort SE-IP
---- -
0001: 0x00000001 0x00000000 0x0000 0x0000 0xC0A80105 (192.168.1.5)

```

## Weight Assignment Command Example

In the following example, SE 1 has better performing hardware than the SE 2. The administrator wants to have more buckets claimed by the SE 1. The following shows that a higher weight number is assigned to the service engine that has better equipment:

```
SE 1(config)# wccp service-number 91 router-list-num 1 port-list-num 1 application cache
weight 1000
```

```
SE 2(config)# wccp service-number 91 router-list-num 1 port-list-num 1 application cache
weight 9000
```

Check the results by entering the following **show** command:  
ServiceEngine# **show ip wccp 91 detail**

```

WCCP Client information:
WCCP Client ID: 192.168.1.5
Protocol Version: 2.0
State: Usable
Redirection: GRE
Packet Return: GRE
Assignment: HASH
Initial Hash Info: 00000000000000000000000000000000
 00000000000000000000000000000000

```

## Web Caching Command Examples

When WCCP support is enabled on the router and on the Service Engines, the devices can communicate and deliver the services for which they are configured. To suspend these services, you can disable WCCP support on the router rather than powering off or otherwise disabling individual Service Engines. (For instance, use the **no ip wccp** router command to disable WCCP support on the router.)

Many WCCP Version 2 services also require a configuration of the appropriate **wccp** global configuration command. Refer to the [Cisco ECDS Command Reference](#).

See the following sections for more information:

- [Web Cache Service Configuration with Clients and Service Engine on the Same Subnet, page 7-25](#)
- [Configuring the Service Engine for Web Cache Service—Clients and Service Engine on the Same Subnet, page 7-25](#)
- [Configuring the Router for Web Cache Service—Clients and Service Engine on the Same Subnet, page 7-25](#)
- [Configuration Examples—Web Cache Service with Clients and Service Engine on the Same Subnet, page 7-26](#)
- [Web Cache Service Configuration with Clients and Service Engine on Different Subnets, page 7-27](#)
- [Configuring the Service Engine for Web Cache Service—Clients and Service Engine on Different Subnets, page 7-27](#)
- [Configuring the Router for Web Cache Service—Clients and Service Engine on Different Subnets, page 7-27](#)
- [Configuration Examples—Web Cache Service with Clients and Service Engine on Different Subnets, page 7-29](#)

## Web Cache Service Configuration with Clients and Service Engine on the Same Subnet

In this scenario, the Service Engine and the requesting clients are on the same subnet. A router running WCCP Version 2 transparently redirects client HTTP traffic bound for router interface s0/0 to the Service Engine. The web cache service redirects HTTP traffic on port 80 only.

### Configuring the Service Engine for Web Cache Service—Clients and Service Engine on the Same Subnet

To configure the Service Engine for web cache service, perform the following steps while logged in to the ECDS software in global configuration mode:

|        | Command                                                        | Purpose                                                                                                  |
|--------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Step 1 | ServiceEngine(config)# <b>wccp version 2</b>                   | Ensures that the Service Engine is running WCCP Version 2.                                               |
| Step 2 | ServiceEngine(config)# <b>wccp router-list 1 10.10.10.1</b>    | Configures a router list.                                                                                |
| Step 3 | ServiceEngine(config)# <b>wccp web-cache router-list-num 1</b> | Informs the routers in the specified router list that the Service Engine is accepting web cache service. |
| Step 4 | ServiceEngine(config)# <b>exit</b>                             | Exits global configuration mode.                                                                         |
| Step 5 | ServiceEngine# <b>copy running-config startup-config</b>       | Writes running configurations to nonvolatile memory.                                                     |

### Configuring the Router for Web Cache Service—Clients and Service Engine on the Same Subnet

To configure the router for web cache service, perform the following steps while logged in to the router in global configuration mode:

|               | Command                                                  | Purpose                                                                                                                                                                                                                                        |
|---------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>ip wccp web-cache</b>                 | Instructs the router to run the web cache service.                                                                                                                                                                                             |
| <b>Step 2</b> | Router(config)# <b>interface Ethernet0</b>               | Specifies which router interface to configure. In this scenario, Ethernet0 is the router interface to which the Service Engine and clients are connected.                                                                                      |
| <b>Step 3</b> | Router(config-if)# <b>ip route-cache same-interface</b>  | Enables fast switching of redirected packets back through the interface on which they were received. Without this command, the router does not use the high-speed switching cache, and the packets are process-switched, a much slower method. |
| <b>Step 4</b> | Router(config)# <b>interface Serial0</b>                 | Specifies which router interface to configure. In this scenario, Serial0 is the router interface to the Internet.                                                                                                                              |
| <b>Step 5</b> | Router(config-if)# <b>ip wccp web-cache redirect out</b> | Instructs the router to redirect web cache traffic bound for the specified interface to Service Engines that accept web cache service. In this scenario there is only one router. Web cache traffic is defined as TCP port 80 traffic.         |
| <b>Step 6</b> | Router(config-if)# <b>exit</b>                           | Exits interface configuration mode.                                                                                                                                                                                                            |

## Configuration Examples—Web Cache Service with Clients and Service Engine on the Same Subnet

This example shows a Service Engine and router configured for web cache service:

### Service Engine

```
hostname Service_engine_2.5.5
!
clock timezone pst -8 0
!
ip domain-name cu.net
!
interface FastEthernet 0
ip address 10.10.20.10 255.255.255.0
no autosense
bandwidth 100
full-duplex
exit
interface FastEthernet 1
shutdown
exit
!
ip default-gateway 10.10.20.1
!
ip name-server 10.10.10.100
!
!
!
wccp router-list 1 10.10.20.1
wccp web-cache router-list-num 1
wccp version 2
!
```

### WCCP-Enabled Router

```
Building configuration...
```

```

Current configuration:
!
version 12.0
!
hostname WCCP-Router
!
!
ip wccp web-cache
!
interface Ethernet0
 ip address 10.10.10.1 255.255.255.0
 ip route-cache same-interface
!
interface Serial0
 ip address 192.168.1.2 255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
 ip wccp web-cache redirect out
!
end

```

## Web Cache Service Configuration with Clients and Service Engine on Different Subnets

In this scenario, the Service Engine and the requesting clients are on different subnets. A router running WCCP Version 2 transparently redirects client HTTP traffic bound for router interface s0/0 to the Service Engine. The web cache service redirects HTTP traffic on port 80 only.

### Configuring the Service Engine for Web Cache Service—Clients and Service Engine on Different Subnets

To configure the Service Engine for web cache service, perform the following steps while logged in to the ECDS software in global configuration mode:

|        | Command                                                        | Purpose                                                                                                  |
|--------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Step 1 | ServiceEngine(config)# <b>wccp version 2</b>                   | Ensures that the Service Engine is running WCCP Version 2.                                               |
| Step 2 | ServiceEngine(config)# <b>wccp router-list 1 10.10.20.1</b>    | Configures a router list.                                                                                |
| Step 3 | ServiceEngine(config)# <b>wccp web-cache router-list-num 1</b> | Informs the routers in the specified router list that the Service Engine is accepting web cache service. |
| Step 4 | ServiceEngine(config)# <b>exit</b>                             | Exits global configuration mode.                                                                         |
| Step 5 | ServiceEngine# <b>copy running-config startup-config</b>       | Writes running configurations to nonvolatile memory.                                                     |

### Configuring the Router for Web Cache Service—Clients and Service Engine on Different Subnets

To configure the router for web cache service, perform the following steps while logged in to the router in global configuration mode:

|        | Command                                  | Purpose                                            |
|--------|------------------------------------------|----------------------------------------------------|
| Step 1 | Router(config)# <b>ip wccp web-cache</b> | Instructs the router to run the web cache service. |

|               |                                                          |                                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | Router(config)# <b>interface Serial0</b>                 | Specifies which router interface to configure. In this scenario, Serial0 is the router interface to the Internet.                                                                                                                          |
| <b>Step 3</b> | Router(config-if)# <b>ip wccp web-cache redirect out</b> | Instructs the router to redirect web cache traffic bound for the specified interface to Service Engines that accept web cache service. In this scenario there is only one router. Web cache traffic is defined as HTTP packets on port 80. |
| <b>Step 4</b> | Router(config-if)# <b>exit</b>                           | Exits interface configuration mode.                                                                                                                                                                                                        |

## Configuration Examples—Web Cache Service with Clients and Service Engine on Different Subnets

This example shows a Service Engine and router configured for web cache service:

### Service Engine Configuration

```
hostname Service_engine_2.5.5
!
clock timezone pst -8 0
!
ip domain-name cisco.com
!
exec-timeout 20
!
interface FastEthernet 0
ip address 10.10.20.10 255.255.255.0
no autosense
bandwidth 100
full-duplex
exit
interface FastEthernet 1
shutdown
exit
!
ip default-gateway 10.10.20.1
!
ip name-server 10.10.10.100
!
!
wccp router-list 1 10.10.20.1
wccp web-cache router-list-num 1
wccp version 2
!
!
!
...
```

### WCCP-Enabled Router Configuration

Building configuration...

Current configuration:

```
!
hostname WCCP-Router
!
!
ip subnet-zero
!
ip wccp web-cache
!
interface Ethernet0
ip address 10.10.10.1 255.255.255.0
!
interface Ethernet1
ip address 10.10.20.1 255.255.255.0
!
interface Serial0
ip address 192.168.1.2 255.255.255.252
no ip directed-broadcast
no ip mroute-cache
ip wccp web-cache redirect out
end
```

## Where to Go Next

Proceed to [Chapter 8, “Configuring Services”](#) for information about configuring ECDS delivery services and programs.

For more information about WCCP, see the following resources:

- [Web Cache Communication Protocol v2](#)

**Tip**

---

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Configuration Guide on Cisco.com.

---





## CHAPTER 8

# Configuring Services

---

The following sections describe how to configure the ECDS:

- [Configuring Delivery Services, page 8-1](#)
- [Configuring Programs, page 8-25](#)
- [Viewing Programs, page 8-37](#)
- [Copying a Program, page 8-39](#)
- [Where to Go Next, page 8-40](#)

## Configuring Delivery Services

Delivery services are configured for prefetch ingest, hybrid ingest, and live programs. Dynamic ingest, the other type of ingest, is dynamically cached upon retrieving content that is not locally stored. For more information about content ingest types, see the [“Ingest and Distribution” section on page 1-4](#).

Configuring a delivery service consists of defining the following:

- [Content Origins](#)
- [Creating Delivery Service](#)
- [Identifying Content](#)

## Content Origins

Content is stored on origin servers. Each delivery service is configured with one origin server. The same origin server can be used by multiple live delivery services. However, only one prefetch/caching delivery service is allowed per origin server.



### Note

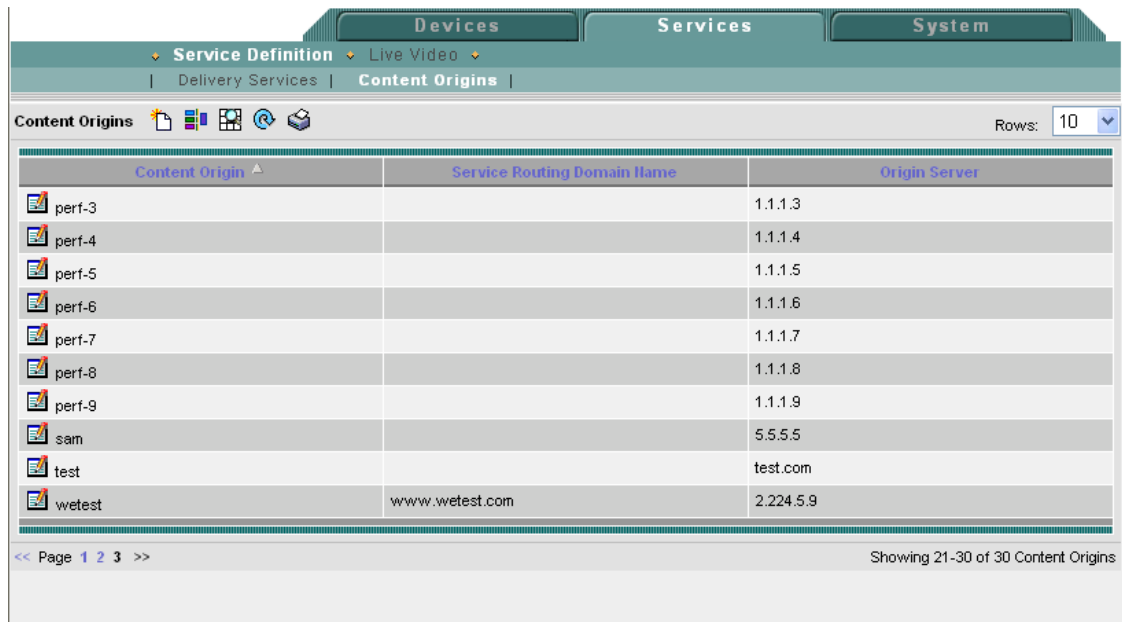
When creating a live delivery service with the same Content Origin as a prefetch/caching delivery service, the same set of SEs must be assigned to both; otherwise, the SR may redirect requests to unassigned SEs.

For more information about origin servers, see the [“Origin Servers” section on page 2-10](#).

To create a Content Origin:

- Step 1** Choose **Services > Service Definition > Content Origins**. The Content Origin Table page is displayed (Figure 8-1).

**Figure 8-1** Content Origin Table Page



| Content Origin | Service Routing Domain Name | Origin Server |
|----------------|-----------------------------|---------------|
| perf-3         |                             | 1.1.1.3       |
| perf-4         |                             | 1.1.1.4       |
| perf-5         |                             | 1.1.1.5       |
| perf-6         |                             | 1.1.1.6       |
| perf-7         |                             | 1.1.1.7       |
| perf-8         |                             | 1.1.1.8       |
| perf-9         |                             | 1.1.1.9       |
| sam            |                             | 5.5.5.5       |
| test           |                             | test.com      |
| wetest         | www.wetest.com              | 2.224.5.9     |

- Step 2** Click the **Create New** icon in the task bar. The Content Origin page is displayed (Figure 8-2).

**Figure 8-2** Content Origin Page

The screenshot shows the 'Content Origin Page' in the Cisco ECDS 2.5 Software Administration Guide. The page is titled 'Creating new Content Origin'. It features a sidebar on the left with a 'Definition' tab. The main content area is divided into sections: 'Content Origin Information' and 'Comments'. The 'Content Origin Information' section contains the following fields:

- Name:** A text input field with a red asterisk indicating it is required.
- Origin Server:** A text input field with a red asterisk indicating it is required.
- Service Routing Domain Name:** A text input field.
- Windows Media Authentication Type:** A dropdown menu currently set to 'None'.

Below these fields is a 'Comments' section with a large text area. At the bottom of the form, there is a note: 'Note: \* - Required Field'. The bottom right corner contains 'Submit' and 'Cancel' buttons.



**Tip** To edit a Content Origin, click the **Edit** icon next to the Content Origin name.

**Step 3** Enter the settings as appropriate. See [Table 8-1](#) for a description of the fields.

**Table 8-1** Content Origin Fields

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                              | Unique name of the origin server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Origin Server                     | Fully qualified domain name (FQDN) of the origin server.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Service Routing Domain Name       | <p>The FQDN to route client requests. The SE translates the service routing domain name (SRDN) to the origin server whenever it needs to retrieve content from the origin server.</p> <p>The service routing domain name configured for the Content Origin should also be configured in the DNS servers, so client requests can get redirected to a Service Router for request mediation and redirection.</p> <p>The URLs that are published to the users have the service routing domain names as the prefix.</p> |
| Windows Media Authentication Type | <p>The type of client authentication that is required by the origin server. The options are:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Basic authentication</li> <li>• NTLM authentication</li> <li>• Digest</li> <li>• Negotiate</li> </ul>                                                                                                                                                                                                                                                    |
| Comments                          | Information about the Content Origin.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Step 4** Click **Submit** to save the settings.



**Tip**

To delete a Content Origin, from the Content Origin Table page, click the **Edit** icon next to the Content Origin you want to delete, and click the **Delete** icon in the task bar.



**Caution**

Do not delete a Content Origin that has a delivery service associated with it. First delete the delivery service associated with the Content Origin, then delete the Content Origin.

## Creating Delivery Service

A delivery service is configured to define how content is acquired, distributed, and stored in advance of a client request.



**Note**

Before creating delivery services, make sure the devices that participate in the delivery service are configured for the type of content to be delivered.

Configure delivery service in the following order:

1. [Create a Service Definition, page 8-4](#)
2. [Configure General Settings, page 8-7](#)
3. [Configure Authorization Service, page 8-8](#)
4. [Configure SE and Content Acquirer Assignment or Device Group and Content Acquirer Assignment, page 8-8](#)
5. [Identifying Content, page 8-10](#)

For more information about delivery services, see the “[Delivery Service](#)” section on page 2-3 of [Chapter 2, “Network Design.”](#)

For information about testing a delivery service, see [Appendix E, “Verifying the Enterprise CDS.”](#)

## Create a Service Definition

**Step 1** Choose **Services > Service Definition > Delivery Services**. The Delivery Services Table page is displayed.

**Step 2** Click the **Create New** icon in the task bar. The Delivery Services Definition page is displayed ([Figure 8-3](#)).



**Tip**

To edit a delivery service, click the **Edit** icon next to the delivery service name.

**Step 3** Enter the settings as appropriate.

**Figure 8-3**      **Delivery Services**

| Delivery Service information                       |                                                                                                                                                                                    |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name:                                              | wwb3-cdn                                                                                                                                                                           |
| Service Routing Domain Name:                       | wa-wwb3.dmsbuecds.com                                                                                                                                                              |
| Origin Server:                                     | winxp2.dmsbuecds.com                                                                                                                                                               |
| Content Origin:                                    | wwb3-orig <a href="#">Edit content origin</a>                                                                                                                                      |
| Live Delivery Service:                             | false                                                                                                                                                                              |
| Delivery Service Quota:                            | 10000 MB                                                                                                                                                                           |
| Acquisition and Distribution Properties            |                                                                                                                                                                                    |
| Distribution Priority:                             | Medium <input type="button" value="v"/> Use null cipher for Distribution: <input type="checkbox"/>                                                                                 |
| Content Acquirer failover/fallback grace period:   | 120 mins <input type="button" value="v"/> Never <input type="checkbox"/> <small>If there is only one SE in root location or if 'Never' is selected, failover/fallback will</small> |
| Use system-wide settings for QoS for unicast data: | <input checked="" type="checkbox"/> <small>System-wide QoS settings page is under the Systems Tab.</small>                                                                         |
| QoS value for unicast data:                        | Default <input type="button" value="v"/> or <input type="text" value="0"/> <small>Select DSCP from the drop-down or enter decimal value in the text box.</small>                   |
| QoS value for content delivery:                    | Default <input type="button" value="v"/> or <input type="text" value="0"/> <small>Select DSCP from the drop-down or enter decimal value in the text box.</small>                   |
| Comments                                           |                                                                                                                                                                                    |

Table 8-2 describes Delivery Service fields.

**Table 8-2**      **Delivery Service Definition Fields**

| Field                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Delivery Service Information</b>            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Name                                           | Unique name for the delivery service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Content Origin                                 | All Content Origins that have been created are listed in the drop-down list. The delivery service and the Content Origin have a one-to-one relationship. To create a new Content Origin, click <b>New Content Origin</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Live Delivery Service                          | <p>Required for WMT Live and MS Live.</p> <p>When checked, creates a live program to distribute live or scheduled programs to the SEs associated with this delivery service and with the live program. This delivery service does not have a related Manifest file and cannot be used to distribute file-based content as regular delivery services do. The live program learns about a live stream through a program file that describes the attributes of the program.</p> <p>Checking this check box disables the Delivery Service Quota field and fields in the Acquisition and Distribution Properties section.</p> <p><b>Note</b> Do not enable Live Delivery Service for Flash Live delivery service.</p> |
| Delivery Service Quota                         | Maximum content storage size, in megabytes, for prefetched content and metadata, and hybrid metadata for this delivery service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Acquisition and Distribution Properties</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Distribution Priority                          | <p>Content distribution priority setting. Options are High, Normal, and Low. The default is Normal.</p> <p>The priority of content acquisition also depends on the origin server. Requests from different origin servers are processed in parallel. Requests from the same origin server are processed sequentially by their overall priority.</p>                                                                                                                                                                                                                                                                                                                                                               |

**Table 8-2**      **Delivery Service Definition Fields (continued)**

| Field                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use null cipher for Distribution                  | When checked, disables encryption for distribution.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Content Acquirer failover/fallback grace period   | Number of minutes before a Content Acquirer failover or a temporary Content Acquirer fallback occurs. The range is from 20 to 120 minutes. For more information, see the “ <a href="#">Content Acquirer Redundancy</a> ” section on page 1-32.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Never                                             | When checked, SE failover or fallback never occurs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Use system-wide settings for QoS for unicast data | <p>When checked, applies the system-wide QoS settings for unicast data to the delivery service. The unicast data refers to the ingest and distribution traffic among SEs.</p> <p>To override the system-wide QoS settings with delivery service-specific QoS values, leave this check box unchecked, and configure the delivery service-specific QoS values in the QoS value for unicast data field.</p> <p>Use the following commands to manage QoS:</p> <ul style="list-style-type: none"> <li>• <a href="#">qos</a>—Globally configures QoS on the device</li> <li>• <a href="#">show qos</a>—Displays QoS information</li> <li>• <a href="#">show statistics qos</a>—Displays statistics for QoS policy service</li> </ul> |
| QoS value for unicast data                        | <p>Configures a Differentiated Services Code Point (DSCP) value for the QoS. The unicast data refers to the ingest and distribution traffic among SEs.</p> <p>If you choose <b>Other</b>, enter a decimal value in the corresponding field.</p> <p>You can set QoS settings on a per-delivery service basis and a system-wide global configuration basis. Delivery service settings take precedence over global settings.</p>                                                                                                                                                                                                                                                                                                  |
| QoS value for content delivery                    | <p>Configures a Differentiated Services Code Point (DSCP) value for the QoS on a per-delivery service basis. Content delivery refers to the traffic the SEs serve to clients.</p> <p>If you choose <b>Other</b>, enter a decimal value in the corresponding field.</p> <p><b>Note</b> This feature applies only to Windows Media Streaming and Web engines. You cannot have a cache hit/miss delivery service and a live delivery service for the same delivery service definition when using the <b>QoS value for content delivery</b> setting.</p>                                                                                                                                                                           |
| Comments                                          | Information about the delivery service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Step 4** Click **Submit** to save the settings.

To delete a delivery service, from the Delivery Service Table page, click the **Edit** icon next to the delivery service you want to delete, and click the **Delete** icon in the task bar.

**Step 5** Continue by defining [Configure General Settings](#).

## Configure General Settings

- Step 1** From the left-panel menu, click **General Settings**. The General Settings page is displayed.
- Step 2** In the **Maximum Bitrate Limit per Session for HTTP** field, enter the maximum rate, in Kbps, at which a client can receive content. The default is 1000.
- This bit rate applies to content that is stored locally, specifically, prefetched, hybrid, or cached. For a cache miss, content is delivered at the rate the origin server sends it.
- Step 3** In the **Maximum Bitrate Limit per Session for HTTP Cache Miss** field, enter the maximum rate, in Kbps, at which a client can receive content that was a cache miss.
- This bit rate applies to content that is not stored locally, specifically, content requiring dynamic caching from the origin server or another SE in the delivery service that has the content.
- Step 4** In the **Disable HTTP Download** field, check the check box to not allow clients to download HTTP content through this delivery service.
- This option disables all HTTP-based content serving from this delivery service. The Web Engine returns a 403 forbidden message.


**Note**

Because the Web Engine receives all HTTP(S) requests before either Windows Media Streaming or Flash Media Streaming, if you disable HTTP(S) download for a Windows Media Streaming delivery service or a Flash Media Streaming delivery service, and a client uses an HTTP(S) request to download the SWF file, the Web Engine returns a 403 forbidden message.

- Step 5** Check the **Enable streaming over HTTP** check box and specify the file types in the **HTTP Allowed Extensions** field to configure progressive download or streaming for certain media files. This setting applies only to the following file types: .asf, none, .nsc, .wma, .wmv, and nsclg.


**Note**

The **Enable streaming over HTTP** check box should be checked if content origin for this delivery service is used for a live program as well.

This delivery service setting has priority over the Windows Media Streaming engine settings on the Service Engines. If Windows Media Streaming is enabled on the Service Engines, and the media types are specified in the HTTP Allowed Extensions field, the delivery service streams the media types specified. If Windows Media Streaming is not enabled, or the media types are not specified in the HTTP Allowed Extensions field, the delivery service uses HTTP download.

- Step 6** In the **Outgoing Cookie** field, enter the cookie if required by the origin server. Some origin servers allow or deny a request based on the cookie included in the request header. If a cookie is configured, all outgoing requests from the SE to the origin server include the configured cookie in the request header.
- Step 7** Click **Submit** to save the settings.


**Tip**

To remove the settings from the delivery service, click the **Remove Settings** icon in the task bar.

- Step 8** Continue by configuring [Configure Authorization Service](#).

## Configure Authorization Service

The Authorization Service page allows you to upload an XML configuration file to allow or deny client requests based on the client's IP address. See the [“Configuring the Authorization Service” section on page 5-18](#) for more information. For more information on the XML configuration file for the Authorization Service, see [Appendix D, “Creating Authorization Service Files.”](#)

- 
- Step 1** From the left-panel menu, click **Authorization Service**. The Authorization Service page is displayed.
- Step 2** Click the **Browse** button to locate the XML configuration file. The Choose File dialog box is displayed. Navigate to the file and click **Open**.
- To remove the configuration file, click the **Delete** icon next to the Config File field name or click the **Delete** icon in the Task bar.
- To validate the file, click the **Validate** button. If there is an error, a dialog box displays information about the error. If there are no errors, the filename and upload time of the XML configuration file are displayed.
- Step 3** Click **Submit**. The XML configuration file is validated. If there is an error, a dialog box displays information about the error. If there are no errors, the filename and upload time of the XML configuration file are displayed.
- To remove the settings from the delivery service, click the **Remove Settings** icon in the task bar.
- 

## Configure SE and Content Acquirer Assignment or Device Group and Content Acquirer Assignment

[Step 1](#) through [Step 4](#) use the Assign Service Engines option to describe the procedure of assigning the Service Engines to the delivery service and selecting one of them as the Content Acquirer. If you have device groups defined, you can use the Assign Device Groups option instead. To assign device groups, follow [Step 1](#) through [Step 4](#) and substitute Device Groups for each instance of Service Engines or SE.



---

**Note** Use either Assign Service Engines, or Assign Device Groups to assign Service Engines and select a Content Acquirer.

---

- 
- Step 1** From the left-panel menu, click **Assign Service Engines**. The Service Engine Assignment page is displayed ([Figure 8-4](#)).



**Figure 8-4** Service Engine Assignment Page

| Service Engine | Unreserved Content Cache (MB) | Total Content Cache (MB) | Status  | Location             | Primed                   |
|----------------|-------------------------------|--------------------------|---------|----------------------|--------------------------|
| NE-612-12      | 134942                        | 139942                   | Online  | NE-612-12-location   | <input type="checkbox"/> |
| NE-612-5       | 119457                        | 119457                   | Online  | tier-1               | <input type="checkbox"/> |
| NE-612-6       | 114942                        | 139942                   | Online  | NE-612-12-location   | <input type="checkbox"/> |
| NE-612-7       | 139942                        | 139942                   | Online  | tier-1               | <input type="checkbox"/> |
| NE-7326-2      | 119323                        | 119423                   | Online  | tier-3               | <input type="checkbox"/> |
| Q5-CDE200-1    | 5238788                       | 5244888                  | Offline | tier-1               | <input type="checkbox"/> |
| Q5-CDE200-2    | 4668080                       | 4768080                  | Offline | Q5-CDE200-2-location | <input type="checkbox"/> |
| Q5-CDE200-4    | 5234888                       | 5244888                  | Online  | tier-1               | <input type="checkbox"/> |
| Q6-CDE200-1    | 1330424                       | 1430424                  | Offline | Q6-CDE200-1-location | <input type="checkbox"/> |
| RT-612-3       | 109801                        | 109801                   | Offline | tier-1               | <input type="checkbox"/> |

**Step 2** Click the **Assign** icon (blue X) next to the SE you want to assign to this delivery service. Alternatively, in the task bar, click **Assign All Service Engines**. The SE assignment states are described in [Figure 8-5](#).

**Figure 8-5** SE Assignment State

|            |                                 |                      |                               |                                                                                            |
|------------|---------------------------------|----------------------|-------------------------------|--------------------------------------------------------------------------------------------|
| New Assign | Assigned and waiting for Submit | Assignment Submitted | Unassign Submitted Assignment | Not modifiable. The quota on all the delivery services for this SE exceeds the disk space. |
|            |                                 |                      |                               |                                                                                            |

A green arrow wrapped around the blue X indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon.

**Step 3** From the **Assign Content Acquirer** drop-down list in the task bar, choose an SE to be the Content Acquirer for this delivery service.

The list contains all SEs currently assigned to the delivery service.

The **Primed** check box indicates if an SE is primed with a live stream. For more information about priming, see the [“Priming a Live Delivery Service”](#) section on page 8-32.

**Step 4** Click **Submit** to save the SE and Content Acquirer assignments.

A green circle with a check mark indicates an SE is assigned to this delivery service. To unassign the SE, click this icon, or click **Unassign All Service Engines** in the task bar. Click **Submit** to save the changes.

**Tip**

To view all the Service Engines assigned to the delivery service, in the left-panel menu, click **List assigned Service Engines**.

**Step 5** Continue by [Identifying Content](#).

## Identifying Content

Content items are identified within the delivery service configuration for prefetch and hybrid ingests. Live program content is identified through the Live Program page, and therefore does not have content items listed for it in the delivery service. The procedures outlined in this section take you through adding content for the delivery service and assumes you have already defined the delivery service (see the [“Creating Delivery Service” section on page 8-4](#)).

**Note**

---

The recommended maximum number of prefetched content items is 200,000.

---

When you configure a delivery service for content acquisition, you must choose one of the following methods:

- [Identifying Content Using the CDSM](#)

The CDSM provides a user-friendly interface that you can use to add content items and specify crawl tasks without having to create and update a Manifest file. The CDSM automatically validates all user input and generates an XML-formatted Manifest file in the background that is free of syntax errors.

Only one Manifest file is generated per delivery service for all content items. You can save your CDSM-generated Manifest file to any accessible location.

- [Identifying Content Using a Manifest File](#)

The externally hosted Manifest files contain the XML tags, subtags, and attributes that define the parameters for content ingest. You must be familiar with the structure of the XML-based Manifest file and be sure the XML tags are properly formatted and syntactically correct before you can create and use Manifest files effectively.

To verify that the content has been acquired, after you have configured the content acquisition method, see the [“Verifying Content Acquisition” section on page 8-25](#).

## Identifying Content Using the CDSM

There are several options for identifying content to be acquired using the CDSM. You can do any of the following:

- Identify a single content item.
- Define a crawl task that searches the origin server at the specified location (URL) and to the specified link depth, and create a list of all content that meets those specifications.
- Define a crawl task with the specifications described in the bullet above, and in addition specify content acquisition rules that further narrow the search.
- Select individual items by performing a quick crawl, and select the items from the crawl result list to be included in the content list.

Table 8-3 describes the icons for identifying content using the CDSM.

**Table 8-3 Delivery Service Content Icons**

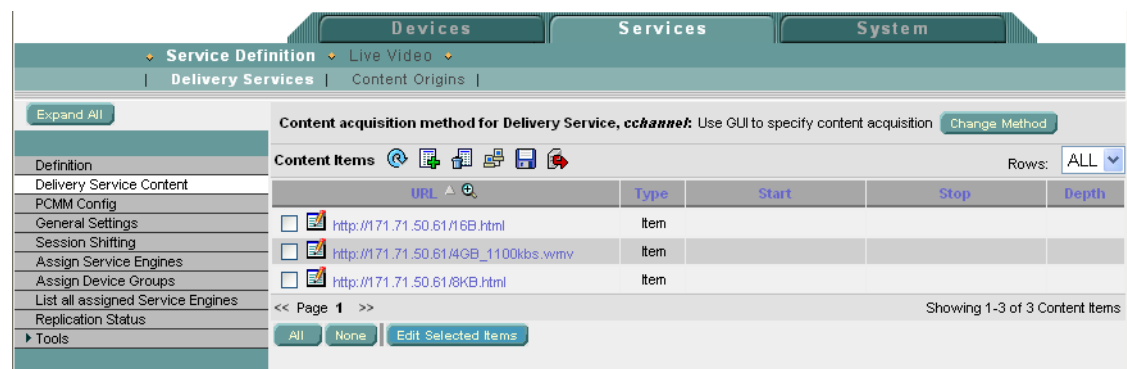
| Icon                                                                                | Function                                                                         |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
|    | Refreshes the table.                                                             |
|    | Adds a content item for acquisition.                                             |
|    | Deletes a selected item.                                                         |
|    | Manages between host and proxy servers for content acquisition.                  |
|    | Saves to disk.                                                                   |
|    | Processes content changes.                                                       |
|    | Views complete URL (+) or views (-) partial URL that is used to acquire content. |
|    | Edits settings for acquiring content from this URL.                              |
|  | Deletes content item.                                                            |

For more information about the crawler feature, see the “Crawling” section on page 2-11.

To identify content for acquisition using the CDSM:

- Step 1** Choose **Services > Service Definition > Delivery Services > Delivery Service Content**. The Content Table page is displayed with “Use GUI to specify content acquisition” as the method (Figure 8-6).

**Figure 8-6 Content Table Page**



- Step 2** Click the **Add Content** icon in the task bar. The Content Manager page is displayed (Figure 8-7).

**Figure 8-7** Content Manager Page

To edit a content item, click the **Edit** icon next to the content. For more information about manipulating the content items in the Content Table page, see the [“Configuring Proxy Server Settings”](#) section on page 8-19.

- Step 3** Choose a protocol from the **Source URL** drop-down list, and enter the source URL in the associated field.

The source URL is the origin server domain name or IP address, followed by a path, or path and filename, if applicable.



**Note** The URL format for Server Message Block (SMB) servers is:

\\SMB server:port\sharedfolder\filepath

If port is not specified in the URL, the default port, 139, is used. Maximum file size, when using SMB for acquisition, is 2 GB. Symbolic links within exported file systems (SMB or NFS) must contain a relative path to the target file, or the target file should be copied into the exported volume.

- Step 4** Do one of the following:

- To identify a single content item, check the **Single Item** check box, and go to the [“Configuring Advanced Settings”](#) section on page 8-16 in this procedure.
- To define a crawl, uncheck the **Single Item** check box, and in the **Link Depth** field, enter the depth of the links to search. Go to the [“Defining a Crawl Task”](#) section on page 8-13 in this procedure.
- To perform a quick crawl, uncheck the **Single Item** check box, and, in the **Link Depth** field, enter the depth of the links to search. Go to the [“Launching Quick Crawl”](#) section on page 8-15 in this procedure.

The crawler feature starts with the Source URL, identifies every web link in the page, and adds every link to the list of URLs to search, until the links have been followed to the specified depth.

The Link Depth field specifies how many levels of a website to crawl or how many directory levels of an FTP server to search. This is optional. The range is –1 to 2147483636.

If the depth is –1, there is no depth constraint.

If the depth is 0, content is acquired only at the starting URL.

If the depth is 1, content is acquired starting at the URL and includes content the URL references.

---

See the following sections for more information about defining crawl tasks:

- [Defining a Crawl Task, page 8-13](#)
- [Launching Quick Crawl, page 8-15](#)
- [Configuring Advanced Settings, page 8-16](#)
- [Configuring Proxy Server Settings, page 8-19](#)

## Defining a Crawl Task

To define a crawl task:

---

- Step 1** Click the **Define a Crawl Task** radio button.
- Step 2** Do *one* of the following:
- Click **Submit** (or **Update** if you are editing an existing content) to add a crawl task to the delivery service. The local Manifest file is automatically reparsed, changes are detected, and the corresponding content items are acquired or removed.
  - Go to the [“Configuring Advanced Settings” section on page 8-16](#), if applicable.
  - Continue to the next step and create acquisition rules.
- Step 3** Click the **Show Optional Content Acquisition Rules** arrow to further refine the crawl task. The fields in the acquisition rules are displayed ([Figure 8-8](#)), and the arrow becomes the **Hide Optional Content Acquisition Rules** arrow.

**Figure 8-8** Content Manager Page—Acquisition Rules Fields

**Step 4** Enter the settings as appropriate. See [Table 8-4](#) for a description of the fields.

**Table 8-4** Acquisition Rule Fields

| Field        | Description                                                                                                                                                                                                                                                                                               |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MIME Type    | A content item qualifies for acquisition only if its MIME type matches this MIME type (for example, video/mpeg).                                                                                                                                                                                          |
| Extension    | A content item is acquired only if its extension matches this extension.                                                                                                                                                                                                                                  |
| Time Before  | Files that were modified before this time qualify for acquisition. Use the dd-mm-yyyy hh:mm:ss [TMZ] format, where TMZ (the time zone) is optional. UTC is the default. Alternatively, click the <b>Calendar</b> icon to choose a date from the calendar and enter a time, and click <b>Apply</b> .       |
| Time After   | Files that were modified after this time qualify for acquisition. Use the format dd-mm-yyyy hh:mm:ss [TMZ] format, where TMZ (the time zone) is optional. UTC is the default. Alternatively, click the <b>Calendar</b> icon to choose a date from the calendar and enter a time, and click <b>Apply</b> . |
| Minimum Size | Content equal to or larger than this value qualifies for acquisition. Choose <b>MB</b> , <b>KB</b> , or <b>Bytes</b> as the unit of measure. The range is 0 to 2147483636.                                                                                                                                |
| Max Size     | Content equal to or less than this value qualifies for acquisition. Choose <b>MB</b> , <b>KB</b> , or <b>Bytes</b> as the unit of measure. The range is 0 to 2147483636.                                                                                                                                  |

**Step 5** Click **Add** to add the rule to the rules list. An entry is added showing the values under each column heading.



**Note** A maximum of ten rules can be configured for each crawl task.

To modify a content acquisition rule, click the **Edit** icon next to the rule. Once you have finished, click the small **Update** button in the content acquisition rules section to save the edits.

To delete a content acquisition rule, click the **Edit** icon next to the rule. Click the **Delete** button in the content acquisition rules section. The rule is removed from the rules listing.

- Step 6** When you have finished adding and modifying content acquisition rules, do one of the following:
- If this is a new crawl task, click **Submit**.
  - If you are editing an existing crawl task, click **Update**.
  - Go to the [“Configuring Advanced Settings” section on page 8-16](#), if applicable.

## Launching Quick Crawl

Quick Crawl is a utility that automatically crawls websites starting from the specified source URL. You can use this utility when you know only the domain name and not the exact location of the content item. Quick Crawl supports crawling only for HTTP and HTTPS acquisition protocols.

To launch a quick crawl:

- Step 1** Click the **Select Individual Items** radio button and click **Launch Quick Crawl**. The Quick Crawl Filter window is displayed.
- Step 2** Enter the settings as appropriate. See [Table 8-5](#) for a description of the fields.

**Table 8-5 Quick Crawl Filter Fields**

| Field           | Description                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MIME Type       | A content item is listed in the results only if its MIME type matches this MIME type (for example, video/mpeg).                                                                                                        |
| Extension       | A content item is listed only if its extension matches this extension.                                                                                                                                                 |
| Modified After  | A content item is listed only if it was modified after this date. Click the <b>Calendar</b> icon to choose a date from the calendar, or enter the date in mm/dd/yyyy format.                                           |
| Modified Before | A content item is listed only if it was modified before this date. Click the <b>Calendar</b> icon to choose a date from the calendar, or enter the date in mm/dd/yyyy format.                                          |
| Minimum Size    | Content equal to or larger than this value is listed in the results. Choose <b>MB</b> , <b>KB</b> , or <b>Bytes</b> as the unit of measure. The range is 0 to 2147483636.                                              |
| Max Size        | Content equal to or less than this value is listed in the results. Choose <b>MB</b> , <b>KB</b> , or <b>Bytes</b> as the unit of measure. The range is 0 to 2147483636.                                                |
| Link Depth      | How many levels of a website to crawl or how many directory levels of an FTP server to crawl. The range is -1 to 2147483636.<br><br>If entered, the value from the Content Manager page is brought over to this field. |

**Table 8-5 Quick Crawl Filter Fields (continued)**

| Field          | Description                                                                                                           |
|----------------|-----------------------------------------------------------------------------------------------------------------------|
| Max Item Count | The maximum number of content items that is listed in the results. The maximum value is 1000.                         |
| Domain         | The <i>host.domain</i> portion of the source URL. Edit this field to limit the search to a specific host on a domain. |
| Username       | The username to log in to host servers that require authentication.                                                   |
| Password       | The password for the user account.                                                                                    |

- Step 3** Click **Start Quick Crawl** to begin search. The Searching for Content status displays a progress bar and shows the number of items found.
- Click **Show Results** to display the content items before the search is complete.
- Click **Refresh Results** to refresh the progress bar.
- When finished, the search results list the MIME type, size, date modified, and URL of each content item that met the search criteria.
- Step 4** Check the check box next to the content items you want to include in this delivery service. Use the **Row** drop-down list to show all content items, or use the **Page** option at the bottom of the table to go to the next page.
- Alternatively, click **Select All** to select all content items. To deselect all, click **Select None**.
- Step 5** Click **Add Selected** to add all selected content items to the delivery service. The Content Table page is displayed with all the selected content items listed.
- Click **Show Filter** to return to the filter and change the filter settings.
- Step 6** To configure advanced settings for the content items listed, click **All** at the bottom of the Content Table page, and then click **Edit Selected Items**. The Content Manager page is displayed with the Advanced Settings option.

## Configuring Advanced Settings

Advanced settings offer controls on how the content is delivered to the client devices.

To configure the advanced settings:

- Step 1** Click the **Show Advanced Settings** arrow. The Advanced Settings fields are displayed ([Figure 8-9](#)), and the arrow becomes the **Hide Advanced Settings** arrow.



**Figure 8-9** Content Manager Page—Advanced Settings Fields

**Delivery Service: cchannel - Content Manager**

Hide advanced settings

**Content Serving Time**

High priority content: ☐ *If selected, acquisition of this content will take precedence.*

Start serving time:  *Stop serving time:*

**Authentication**

Use weak SSL certificate: ☐ *If selected, allow https protocol to accept expired or self-signed certificate.*

Disable basic authentication: ☐ *If selected, acquirer will not use basic authentication while fetching content.*

Windows Media Playback Authentication:  *Determines whether users need to be authenticated before the specified content is played.*

User name:  Password:

User Domain Name:

**URL Settings**

No redirect to origin server: ☐ *If selected, disallows CDN edge device to redirect content requests to the origin server if the content is not ready at the that device.*

Ignore query string: ☐ *If selected, CDN will ignore any string after "?" in the request url for playback.*

Alternate URL:  *If a content requested by the user is not ready in CDN, the user will be redirected to this URL.*

**Content Settings**

TTL:   *Specify the frequency of re-checking the content. If -1 never, re-checked after initial acquisition.*

Retry interval:   *If acquisition fails, retry in this time period.*

Note: \* - Required Field

**Step 2** Enter the settings as appropriate. See [Table 8-6](#) for a description of the fields.

**Table 8-6** Advanced Settings for Serving Content

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Content Serving Time</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| High Priority Content       | Specifies the importance, and therefore the processing order, of the item acquisition or crawl task.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Start Serving Time          | Specifies the time for the SE to start delivering content. Use the format dd-mm-yyyy hh:mm:ss [TMZ] format, where TMZ (the time zone) is optional. UTC is the default. Alternatively, click the <b>Calendar</b> icon to choose a date from the calendar and enter a time, and click <b>Apply</b> .<br><br>If you do not specify a time, content is ready for delivery as soon as it is acquired and distributed to the SEs in the delivery service.                                                                                                                                                                                                          |
| Stop Serving Time           | Specifies the time for the SE to stop delivering content. Use the dd-mm-yyyy hh:mm:ss [TMZ] format, where TMZ (the time zone) is optional. UTC is the default. Alternatively, click the <b>Calendar</b> icon to choose a date from the calendar and enter a time, and click <b>Apply</b> .<br><br>If you do not specify a time, content continues to be available for delivery until you remove it from the delivery service either by changing the local Manifest file, using the Content Removal page, or renaming the delivery service. For information about the Content Removal page, see the <a href="#">“Removing Content”</a> section on page 11-21. |

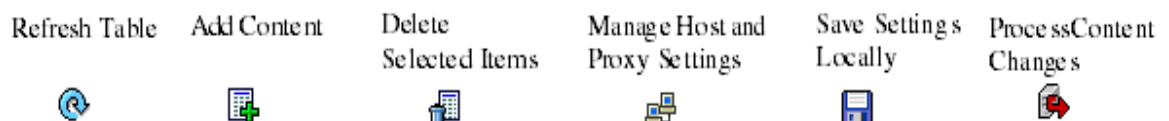
**Table 8-6**      **Advanced Settings for Serving Content (continued)**

| Field                                 | Description                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication</b>                 |                                                                                                                                                                                                                                                                                                                                                                      |
| Use weak SSL certificate              | If checked, allows acceptance of expired or self-signed certificates during authentication.                                                                                                                                                                                                                                                                          |
| Disable basic authentication          | If checked, NTLM headers are not stripped off that would allow fallback to the basic authentication method while acquiring content.                                                                                                                                                                                                                                  |
| Windows Media Playback Authentication | Sets the authentication for Windows Media playback to one of the following: <ul style="list-style-type: none"> <li>As acquired—Requires authentication on playback based on settings from origin server.</li> <li>Require authentication—Requires authentication upon playback.</li> <li>No authentication—Does not require authentication upon playback.</li> </ul> |
| User Name                             | Name of the user for authentication.                                                                                                                                                                                                                                                                                                                                 |
| Password                              | Password of the user for authentication.                                                                                                                                                                                                                                                                                                                             |
| User Domain Name                      | NTLM user domain name for the NTLM authentication scheme.                                                                                                                                                                                                                                                                                                            |
| <b>URL Settings</b>                   |                                                                                                                                                                                                                                                                                                                                                                      |
| Ignore Query String                   | If checked, ignores any string after the question mark (?) character in the requested URL for playback.                                                                                                                                                                                                                                                              |
| <b>Content Settings</b>               |                                                                                                                                                                                                                                                                                                                                                                      |
| TTL                                   | Time period for revalidation of content. Select unit of measure from the drop-down list.<br><br>If no TTL is entered, the content is fetched only once, and its freshness is never checked again.                                                                                                                                                                    |
| Retry Interval                        | Time period in which the Content Acquirer can attempt to acquire the content again if the acquisition fails.                                                                                                                                                                                                                                                         |

- Step 3** Click **Submit** to process the content request. When you click **Submit**, the local Manifest file for this delivery service is automatically reparsed, changes are detected, and the corresponding items are acquired or removed. This action, however, does not trigger a recheck of all the content in the delivery service.

## Content Table

The Content Table page ([Figure 8-11](#)) offers the task bar functions described in [Figure 8-10](#).

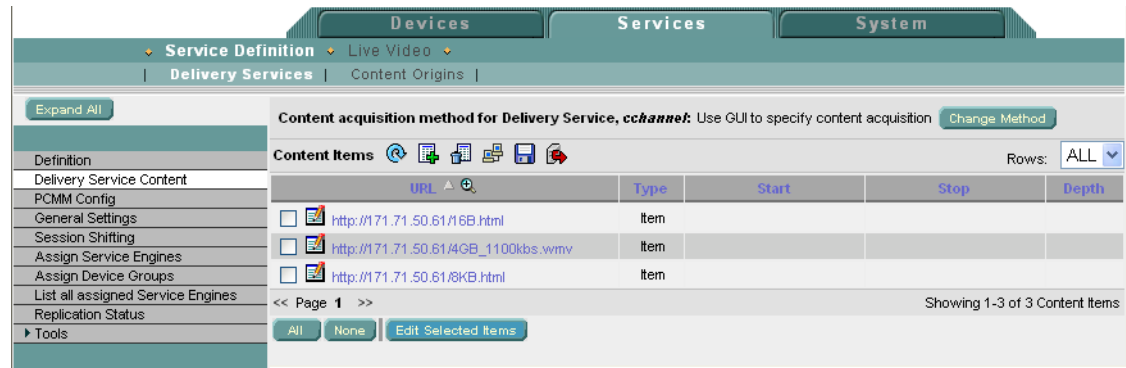
**Figure 8-10**      **Content Table Task Bar Icons**

The **Refresh Table** icon refreshes the content table.

The **Add Content** icon allows you to add content items by displaying the Content Manager page.

To delete a content item, check the check box next to each item you want to delete, and click the **Delete Selected Items** icon. To select all content items, click **All**. To deselect all content items, click **None**.

**Figure 8-11 Content Table Page**



For information on the **Manage Host and Proxy Settings** icon, see the “[Configuring Proxy Server Settings](#)” section on page 8-19.

After you save the CDSM-generated Manifest file by clicking **Submit** in the Content Manager page, you can save the Manifest file locally, and modify it. Choose the content item in the table, and click the **Save Settings Locally** icon in the task bar. A web browser window with the CDSM-generated Manifest file elements is displayed. Choose the **File Save As** option, enter a name for the Manifest file, and click **OK**. The Manifest file is saved on your PC. See [Appendix B, “Creating Manifest Files,”](#) for more information.

To acquire configured content items immediately, click the **Process Content Changes** icon in the task bar.



**Note**

If you change the Manifest file that you saved, and you want to use that Manifest file instead of the content that you defined in the CDSM, or if you want to use the Manifest file for another delivery service, then you must use the **Specify external manifest file** method and point to the Manifest file. When you change the content acquisition method, any content items that you added are removed. For information about the Manifest file, see the “[Identifying Content Using a Manifest File](#)” section on page 8-21 and [Appendix B, “Creating Manifest Files.”](#)

To edit multiple content items, check the check box next to each item you want to edit, and click **Edit Selected Items**.

## Configuring Proxy Server Settings

When the Content Acquirer cannot directly access the origin server, because the origin server is set up to allow access only by a specified proxy server, you can configure acquisition through a proxy server. When a proxy server is configured for the Content Acquirer, the Content Acquirer contacts the proxy server instead of the origin server, and all requests to that origin server go through the proxy server.



**Note**

Content acquisition through a proxy server is supported only for HTTP requests.

**Note**

Before configuring a proxy server, verify that the Content Acquirer is able to ping the proxy server. If the proxy is not servicing the configured port, you will get the message: “failed: Connection refused.”

To configure a proxy server for content items identified using the CDSM:

- Step 1** From the Content Table page, click the **Manage Host and Proxy Settings** icon in the task bar.
- The Content Hosts Table page is displayed, listing all previously created host URLs, the number of content items for each host, and a proxy server (if configured).
- To return to the Content Table page, click **Return to Content Listing**.
- Step 2** Check the check box next to each host you want to configure with a proxy server.
- Step 3** Click **Manage Proxy for Selected Hosts**. The Proxy Server page is displayed.
- Under the Defining Proxy Server for the Following Hosts heading, a bulleted list of host servers is displayed for which proxy servers are being configured.
- Step 4** In the Proxy Server Specifications area, enter the settings as appropriate. See [Table 8-7](#) for a description of the fields.

**Table 8-7 Proxy Server Fields**

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Proxy Host                   | Hostname or IP address of the proxy server used by the Content Acquirer for content acquisition. When you use a domain name instead of an IP address, make sure that the domain name can be resolved by the DNS servers.                                                                                                                                                                      |
| Proxy Port                   | Port number of the proxy server on which the Content Acquirer fetches content. The range is from 1 to 65535.                                                                                                                                                                                                                                                                                  |
| Disable Basic Authentication | When checked, NTLM headers cannot be stripped off that would allow fallback to the basic authentication method.<br><br>If you leave this check box unchecked, NTLM authentication headers can be stripped to allow fallback to the basic authentication method and the username and password information can be passed to the origin server in clear text with a basic authentication header. |
| User Name                    | Name of the user to be authenticated to fetch the content.                                                                                                                                                                                                                                                                                                                                    |
| Password                     | Password of the user to pass authentication from the proxy.                                                                                                                                                                                                                                                                                                                                   |

**Note**

If the specified proxy fails, the Content Acquirer, by default, contacts the origin server directly and tries to fetch the content.

- Step 5** Click **Add** to add the proxy server.
- To edit the proxy server settings, choose the proxy server from the Select a Proxy Server list, and click **Edit**. The values for the proxy server are displayed in the Proxy Server Specification section. Once you have finished modifying the settings, click **Update**.
- To delete the proxy server settings, choose the proxy server from the Select a Proxy Server list, and click **Delete**.

- Step 6** To assign the proxy server to the host or hosts listed on this page, choose a proxy server from the Select a Proxy Server list, and click **Save Assignment**. The Content Hosts Table page is displayed.
- 

## Identifying Content Using a Manifest File

The Manifest file provides information about the content to be prefetched, or fetched at a later time (as in hybrid ingest), or provides information about live content streamed through the delivery service.

### Before You Begin

Before configuring the CDSM to receive a Manifest file:

1. Create the Manifest file. See [Appendix B, “Creating Manifest Files”](#) for details on creating a Manifest file.
2. After you create the Manifest file, use the Manifest Validator utility to verify the syntax. See the [“Manifest Validator Utility” section on page B-15](#) for more information.

### Procedure

To configure the Manifest file settings:

- 
- Step 1** Choose **Services > Service Definition > Delivery Services > Delivery Service Content**. The Content Table page is displayed with Use GUI to specify content acquisition as the method.
- Step 2** To change to the Specify external Manifest file method:
- a. Click **Change Method**.
  - b. From the drop-down list choose, **Specify external manifest file**.
  - c. Click **Save**.
  - d. In the confirmation dialog box, click **OK**.

The Content Manager page displays the Manifest file settings ([Figure 8-12](#)).



### Note

When you change the content acquisition method from Use the GUI to specify content acquisition to Specify external Manifest file for an existing delivery service, any content items that you added using the CDSM are removed. To save the existing settings, click the **Save Settings Locally** icon in the task bar.

---

**Figure 8-12** Content Manager Page—Manifest File Settings

**Step 3** Enter the settings as appropriate. See [Table 8-8](#) for a description of the fields.

**Table 8-8** Manifest File Settings Fields

| Field                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Define Basic Manifest Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Manifest URL                          | Address of the Manifest file for the delivery service. The Manifest URL must be a well-formed URL. If the protocol (FTP, HTTP, or HTTPS) for the URL is not specified, HTTP is used.<br><br>To validate the Manifest file from this page, click <b>Validate</b> . A new window displays the validation results. For more information, see the “ <a href="#">Manifest Validator Utility</a> ” section on page B-15. |
| Check Manifest Every                  | Frequency, in minutes (0 to 52560000), at which the Content Acquirer assigned to the delivery service checks for updates to the Manifest file.<br><br>To fetch the Manifest file now, click <b>Fetch Manifest Now</b> .                                                                                                                                                                                            |

**Table 8-8 Manifest File Settings Fields (continued)**

| Field                                    | Description                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Weak Certificate Verification            | When checked, enables weak certificate verification for fetching the Manifest file. This is applicable when the Manifest file is fetched using HTTPS.<br><br><b>Note</b> To use weak certification for content ingest, you need to specify weak certification within the Manifest file.                                                                                                |
| Disable Basic Authentication             | When checked, NTLM headers cannot be stripped off to allow fallback to the basic authentication method.<br><br>If you leave this check box unchecked, NTLM authentication headers can be stripped to allow fallback to the basic authentication method, and the username and password information can be passed to the origin server in clear text with a basic authentication header. |
| Manifest Username                        | Username of the account that is allowed to fetch the Manifest file from the server. The Manifest username must be a valid ID. If the server allows anonymous login, the user ID can be null.<br><br><b>Note</b> The Manifest Username and Manifest Password fields allow you to enter any secure login information needed to access the Manifest file at its remote location.          |
| Manifest Password                        | Password for the user.                                                                                                                                                                                                                                                                                                                                                                 |
| Confirm Password                         | Password confirmation.                                                                                                                                                                                                                                                                                                                                                                 |
| NTLM User Domain Name                    | NTLM user domain name to be allowed access by the NTLM authentication scheme configured on the server where the Manifest file is located.                                                                                                                                                                                                                                              |
| <b>Define Manifest Proxy Information</b> |                                                                                                                                                                                                                                                                                                                                                                                        |
| Disable All Proxy                        | Disables the outgoing proxy server for fetching the Manifest file. Any outgoing proxy server configured on the Content Acquirer is bypassed, and the Content Acquirer contacts the server directly. See the <a href="#">“Configuring Web Engine HTTP Connections”</a> section on page 5-39 for information about configuring outgoing HTTP proxy servers.                              |
| Proxy Hostname                           | Hostname or IP address of the proxy server used by the Content Acquirer to retrieve the Manifest file.                                                                                                                                                                                                                                                                                 |
| Proxy Port                               | Port number of the proxy sever where the Content Acquirer fetches the Manifest file. The range is from 1 to 65535.                                                                                                                                                                                                                                                                     |
| Proxy Username                           | Name of the user to be authenticated to fetch the Manifest file.                                                                                                                                                                                                                                                                                                                       |
| Proxy Password                           | Password of the user to pass authentication on the proxy.                                                                                                                                                                                                                                                                                                                              |
| Confirm Password                         | Re-entry of the same password for confirmation to pass authentication on the proxy.                                                                                                                                                                                                                                                                                                    |
| Disable Proxy Basic Authentication       | When checked, NTLM headers are not stripped off to allow fallback to the basic authentication method against Microsoft Internet Information Services (IIS) servers.                                                                                                                                                                                                                    |
| Proxy NTLM User Domain Name              | NTLM user domain name to be allowed access by the NTLM authentication scheme configured on the proxy.                                                                                                                                                                                                                                                                                  |

**Note**

When you configure a proxy server in the Manifest File Settings page, the proxy configuration is valid only for acquiring the Manifest file itself and not for acquiring the delivery service content. Requests for the Manifest file go through the proxy server, whereas requests for content go directly to the origin server.

**Step 4** Click **Submit** to save the settings.

**Step 5** To fetch a new or updated Manifest file, click **Fetch Manifest Now**. You are prompted to confirm your decision.

When you click this button, a process initiates that checks to see if the Manifest file has been updated, and that the updated Manifest file has been downloaded and reparsed. Also, regardless of whether the Manifest file has been updated, all content for the delivery service is rechecked and any new content is ingested, unless the *ttl* attribute in the Manifest file is set to a negative number. For more information, see the [“Refreshing and Removing Content” section on page B-13](#).

**Note**

Content that is removed from the Manifest file is made unavailable as soon as the updated Manifest file is fetched. Obsolete content is not immediately deleted from the delivery service cache, but is eventually removed to make room for new content.

**Step 6** To force the replication of content and refresh the information:

- a. In the left-panel menu, click **Replication Status**. The Replication Status page is displayed.
- b. In the “View Detailed Replication Status for Delivery Service by Device” section, run a search for a selected device. The Replication Items are displayed.
- c. Click the **Force Replication information refresh** icon in the task bar. You are prompted to confirm your decision.

For more information on delivery service replication, see the [“Replication Status for a Delivery Service” section on page 10-30](#).

## Manifest File Proxy Server Settings

There are three ways to configure the proxy server when using a Manifest file to ingest content: through the CDSM, through the CLI, or through the Manifest file. If you need to configure the SE to use the proxy for both caching and prefetched content, use the CLI to configure the proxy. The CLI command is a global configuration command that configures the entire SE to use the proxy. If only the Content Acquirer portion of the SE needs to use the proxy for acquiring prefetched content, use the Manifest file to specify the outgoing proxy. When you configure the proxy server in the Manifest file, you are configuring the Content Acquirer to use the proxy to fetch content for the delivery service.

**Note**

Proxy configurations in the Manifest file take precedence over proxy configurations in the CLI. Furthermore, a *noProxy* configuration in the Manifest file takes precedence over the other proxy server configurations in the Manifest file.



## Verifying Content Acquisition

After you have configured the content acquisition method, you can verify that the content has been ingested by logging in to the SE acting as the Content Acquirer for the delivery service and using the **cdnfs browse** command.

The **cdnfs browse** command is an interactive command and has the following subcommands used to view ECDS network files and directories:

```
ContentAcquirer# cdnfs browse
----- CDNFS interactive browsing -----
dir, ls: list directory contents
cd,chdir: change current working directory
info: display attributes of a file
more: page through a file
cat: display a file
exit,quit: quit CDNFS browse shell
```

The **ls** command lists the websites as directories. File attributes and content can be viewed using the **cdnfs browse** sub-commands.

For more information about the **cdnfs** command, see *Cisco Enterprise CDS 2.5 Command Reference*. For online documentation, see the [“Related Documentation”](#) section on page xxi.

## Configuring Programs

A program in the ECDS is defined as a scheduled live or rebroadcast event that streams content to client devices. The ECDS streams live or rebroadcast content by using the Movie Streamer, Windows Media Streaming, or Flash Media Streaming engine. For more information, see the [“Programs”](#) section on page 2-27.

To view existing programs, see the [“Viewing Programs”](#) section on page 8-37.

Each live program can have up to ten different playtimes scheduled. The program is broadcast from all Service Engines simultaneously.

Flash Media Streaming uses Real Time Media Protocol (RTMP) to stream live content by dynamic proxy. Configuration of live or rebroadcast programs is not required. When the first client requests live streaming content, the stream is created. For more information, see the [“Live Streaming”](#) section on page 1-19.



### Caution

If you have configured delivery services for live programs, make sure there are no external proxy servers physically located between your receiver SEs and your Content Acquirer that require proxy authentication. Also, make sure that proxy authentication is not enabled on any receiver SEs that might be in the logical, hierarchical path between the Content Acquirer and the receiver SE that is going to serve the live stream to the requesting clients. If a live stream encounters any device that requires proxy authentication, the stream is dropped before it reaches its destination.



### Note

All SEs in a Windows Media live delivery service must have Real Time Streaming Protocol with TCP (RTSPT) enabled, because SEs must use the RTSPT protocol to communicate with each other. RTSPT is enabled by default.

**Tip**

For information about testing a live or rebroadcast program, see [Appendix E, “Verifying the Enterprise CDS.”](#)

**Note**

The following rules apply to live splitting for Movie Streamer:

1. For unicast streaming, the client request must be sent by RTSP.
2. For multicast streaming, the client request must be sent by HTTP.

**Multicast Live Stream Interruptions**

During a Windows Media live broadcast, any interruption of the live stream that lasts five minutes or longer causes the multicast broadcast to cease for the duration of the currently scheduled period. If the live stream is interrupted for less than five minutes, the broadcast resumes.

Live stream interruptions can be caused by unexpected encoder failures or by an operational restart. If the live stream stops for more than five minutes and resumes later while the program is still scheduled, you can modify the schedule or any other attribute of the program (such as the description) to trigger a restart of the multicast broadcast. Restarting might take up to five minutes under these circumstances.

This does not apply to unicast delivery of a Windows Media live event or to Movie Streamer live programs.

## Defining a Program

To define a live or rebroadcast program:

**Step 1** Choose **Services > Live Video > Live Programs**. The Program Table page is displayed.

**Step 2** Click the **Create New** icon in the task bar. The Program Definition page is displayed.

**Tip**

To edit an existing program, click the **Edit** icon next to the program name.

**Step 3** In the **Name** field, enter a unique name for the program.

**Step 4** From the **Type** drop-down list, choose a program type.

**Step 5** Check the **Auto Deletion** check box if you want the program to be automatically deleted 24 hours after it has finished. This option only applies to live programs.

**Step 6** In the **Description** field, enter information about the program.

**Step 7** Click **Submit** to save the settings.

You have completed defining the program type. Proceed to the following sections:

- To configure Movie Streamer live and Windows Media live programs, see the next section, [“Configuring Live Programs.”](#)
- To configure Windows Media rebroadcast and Movie Streamer rebroadcast programs, see the [“Configuring a Rebroadcast”](#) section on page 8-33.

For information about copying a program, see the [“Copying a Program” section on page 8-39](#).

---

## Configuring Live Programs

Once you have defined the program type, you must select a live delivery service, configure the streaming, and create a schedule. This procedure takes you through these steps and assumes you have already defined the program (see the [“Defining a Program” section on page 8-26](#)).

To configure a Movie Streamer live or Windows Media live program:

---

**Step 1** After you have chosen a program from the Program Table page, click **Select Live Delivery Service**. The Select Live Delivery Service page is displayed listing all the live delivery services configured.

To set the QoS value for live programs, set the QoS value for the delivery service. See the “Service Definition” section in the [“Creating Delivery Service” section on page 8-4](#) for more information.

**Step 2** Click the radio button next to the name of the live delivery service you want to associate with the program and click **Submit**. Alternatively, click the **Create New Live Delivery Service** icon in the task bar.

If you are creating a new live delivery service, the New Live Delivery Service page is displayed.

- a. The **Name** field is automatically populated with a unique delivery service name. If you wish to change the name given by default, enter a unique name for the delivery service in this field.
- b. From the **Content Origin** drop-down list, choose a Content Origin.
- c. Click **Submit** to save the settings.

### SE and Content Acquirer Assignment or Device Group and Content Acquirer Assignment

[Step 3](#) through [Step 7](#) use the Assign Service Engines option to describe the procedure of assigning the Service Engines to the live program and selecting one of them as the Content Acquirer. If you have device groups defined, you can use the Assign Device Groups option instead. To assign device groups, follow [Step 3](#) through [Step 7](#) and substitute Device Groups for each instance of SE.

**Step 3** From the left-panel menu, choose **Assign Service Engines**. The Service Engine Assignment page is displayed ([Figure 8-13](#)).

**Figure 8-13** Service Engine Assignment Page

Service Engine assignments for Delivery Service, *cchannel* with Quota 100000 MB

Service Engines: Assign Content Acquirer: Q6-CDE200-1 Rows: ALL

| Service Engine | Unreserved Content Cache (MB) | Total Content Cache (MB) | Status  | Location             | Primed                   |
|----------------|-------------------------------|--------------------------|---------|----------------------|--------------------------|
| NE-612-12      | 134942                        | 139942                   | Online  | NE-612-12-location   | <input type="checkbox"/> |
| NE-612-5       | 119457                        | 119457                   | Online  | tier-1               | <input type="checkbox"/> |
| NE-612-6       | 114942                        | 139942                   | Online  | NE-612-12-location   | <input type="checkbox"/> |
| NE-612-7       | 139942                        | 139942                   | Online  | tier-1               | <input type="checkbox"/> |
| NE-7326-2      | 119323                        | 119423                   | Online  | tier-3               | <input type="checkbox"/> |
| Q5-CDE200-1    | 5238788                       | 5244888                  | Offline | tier-1               | <input type="checkbox"/> |
| Q5-CDE200-2    | 4668080                       | 4768080                  | Offline | Q5-CDE200-2-location | <input type="checkbox"/> |
| Q5-CDE200-4    | 5234888                       | 5244888                  | Online  | tier-1               | <input type="checkbox"/> |
| Q6-CDE200-1    | 1330424                       | 1430424                  | Offline | Q6-CDE200-1-location | <input type="checkbox"/> |
| RT-612-3       | 109801                        | 109801                   | Offline | tier-1               | <input type="checkbox"/> |

<< Page 1 >> Showing 1-10 of 10 Service Engines

- Step 4** Click the **Assign** icon (blue X) next to the SE you want to assign to this delivery service. Or, in the task bar, click the **Assign All Service Engines** icon. The SE assignment states are described in [Figure 8-14](#).

**Figure 8-14** SE Assignment State

|            |                                 |                      |                    |                                                                                            |
|------------|---------------------------------|----------------------|--------------------|--------------------------------------------------------------------------------------------|
| New Assign | Assigned and waiting for Submit | Assignment Submitted | Unassign Submitted | Not modifiable. The quota on all the delivery services for this SE exceeds the disk space. |
|            |                                 |                      |                    |                                                                                            |

A green arrow wrapped around the blue X indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon.

- Step 5** From the **Assign Content Acquirer** drop-down list in the task bar, choose an SE to be the Content Acquirer for this live delivery service.
- The list contains all SEs currently assigned to the delivery service.
- Step 6** Check the **Primed** check box for each SE you want to prime with the live stream. For more information about priming, see the [“Priming a Live Delivery Service”](#) section on page 8-32.
- Step 7** Click **Submit** to save the SE and Content Acquirer assignments.
- A green circle with a check mark indicates an SE is assigned to this delivery service. To unassign the SE, click this icon, or click the **Unassign All Service Engines** icon in the task bar. Click **Submit** to save the changes.
- Step 8** In the left-panel menu, choose **Live Streaming**. The Live Stream Settings page is displayed.
- The Live Stream Setting page differs depending on whether you are configuring a Movie Streamer live stream or a Windows Media live stream.
- Step 9** Enter the settings as appropriate. See [Table 8-9](#) for a description of the Windows Media Live Stream Settings fields, and [Table 8-10](#) for a description of the Movie Streamer Live Stream Settings fields.

**Note**

The string “ipfwd” cannot be used as the program name or in the URL because ipfwd is a keyword used in the IP-forwarding feature.

**Table 8-9**      **Windows Media Live Stream Settings Fields**

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Live Source URL                     | <p>The URL of the origin Windows Media encoder or Windows Media server using the following format:</p> <ul style="list-style-type: none"> <li>• http://WMencoder_or_WMStreamerServer:port/path/file</li> <li>• rtsp://WMencoder_or_WMStreamerServer:port/path/file</li> </ul> <p>For encoder failover, you can specify more than one encoder. When multiple live source URLs are entered, the ECDS tries the other sources should one source fail.</p> <p><b>Tip</b>      When you enter multiple live source URLs, separate each entry in the list with a semicolon (;)</p> <p>The WMT component keeps a list of the encoders as entered in the WMT live program specifications. When a request comes in, WMT selects the first configured encoder source and attempts to connect to it. If there is an error in the connection, the encoder status is marked as “dead” and affixed with a time of death.</p> <p>A retry is then performed. WMT goes through its list of encoders again, skipping any dead encoders. If all encoders are marked as dead, WMT retries the oldest dead encoder. This process loops until the client queries for status, at which point an error is returned, and the client-server disconnects.</p> <p>For primed streams (streams where the SE is expected to pre-ingest the stream to improve responsiveness to clients), the Content Acquirer should retry the oldest dead encoder every minute. Only one encoder is tested each time: In the 1st minute, WMT tests encoder 1. If the connection is unsuccessful, it marks encoder 1 as dead and updates the time of death. Then WMT sleeps for 1 minute then continues in the same fashion with encoder 2, and so on.</p> <p><b>Note</b>      If you use a .wsx file as the Live Source URL and specify the encoders within the .wsx files, failover does not work for unicast-in multicast-out. We recommend you use a managed live-based encoder with redundancy, as it supports encoder failure with all type of streams.</p> |
| Enable Unicast Delivery to Client   | If enabled, the program uses unicast transmission.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Unicast URL Reference               | If <b>Enable Unicast Delivery to Client</b> is checked, this field is auto-populated with a list of suggested URLs created from the Origin Server and the Service Routing Domain Name fields associated with the live delivery service. Choose one from the drop-down list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Enable Multicast Delivery to Client | If enabled, the program uses multicast transmission.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Enable Multicast Delivery to SE     | If enabled, multicast transmission is used to distribute content from the Content Acquirer to the SEs. This option is only for multicast-enabled networks. If your network is not enabled for multicast, this feature does not function properly.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Multicast URL Reference             | If <b>Enable Multicast Delivery to Client</b> is checked, this field is auto-populated with a list of suggested URLs created from the Origin Server and the Service Routing Domain Name fields associated with the live delivery service. Choose one from the drop-down list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Table 8-9**      **Windows Media Live Stream Settings Fields (continued)**

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NSC Reference for Multicast | The URL for the NSC file used for a server-side playlist as the media source in a multicast program. This field is available when <b>Enable Multicast Delivery to Client</b> is checked.                                                                                                                                                                                                                 |
| Multicast Address and Port  | The multicast address and port to use for streaming this program using multicast. The address range is 224.0.0.0 to 239.255.255.255. The port number must be even, and within the range of 1 to 65535. These values must be unique within the system.<br><br>Even numbered ports are for Real-Time Transport Protocol (RTP), and odd numbered ports are for Real-Time Transport Control Protocol (RTCP). |
| Multicast TTL               | Specify the multicast time-to-live (number of hops). The default is 15 hops.                                                                                                                                                                                                                                                                                                                             |

**Table 8-10**      **Movie Streamer Live Stream Settings Fields**

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Origin Server SDP File URL | <p><b>Note</b> If you are using an SDP file created by a Cisco Digital Media Encoder, remove the line <b>a=range:npt=0-</b> from the file before performing this step.</p> <p>The URL for the Session Description Protocol (SDP) file generated on the encoder. From the drop-down list, select either <b>rtsp</b> or <b>http</b>, and enter the remainder of the URL in the field. The remainder of the URL format is host [:port]/[filename], where the port and filename are optional. For the Darwin Streaming Server encoder, you need to specify the SDP file. For the Digital Rapid encoder, you do not need to specify the SDP file.</p> <p>When you click the <b>Auto Populate</b> button, the Incoming Live Streams Settings fields (the next section on the Live Streaming Settings page) are automatically populated based on the Origin Server SDP File URL.</p> |
| Backup SDP URL             | <p>The backup URL for the SDP file. This field is only for RTSP. Add a valid backup URL and click <b>Auto Populate</b>. The Incoming Live Streams Settings backup fields (the next section on the Live Streaming Settings page) are automatically populated based on the Backup SDP URL.</p> <p>The Cisco ECDS only supports failover between a primary origin server and a backup origin server for a Movie Streamer live program when the backup origin server uses the same codec as the primary.</p> <p>When you click the <b>Auto Populate</b> button, the Incoming Live Streams Settings fields (the next section on the Live Streaming Settings page) are automatically populated based on the Backup SDP URL.</p>                                                                                                                                                     |

**Incoming Live Streams Settings**

**Note** Manually enter these fields when Auto Populate cannot parse the SDP URL.

|                      |                                                                                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source Server        | The stream source IP address.                                                                                                                                                                                                                              |
| Backup Source Server | The backup stream source IP address.                                                                                                                                                                                                                       |
| Receiving IP         | <p>For RTSP, the Primary Receiving IP is the IP address of the Content Acquirer acting as the primary receiver. This is always unicast-in.</p> <p>For HTTP, the Primary Receiving IP is the multicast-in IP address used to broadcast the live stream.</p> |

**Table 8-10** *Movie Streamer Live Stream Settings Fields (continued)*

| Field                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup Receiving IP                   | For RTSP, the Backup Receiving IP is the IP address of the Content Acquirer acting as the backup receiver. Both the primary and backup Content Acquirer are located in the root location of the delivery service.<br><br>For HTTP, the Backup Receiving IP is the multicast-in IP address used to broadcast the live stream.                                                                                                |
| Receiving Ports                       | Receiving Ports are used to define each port related to audio and video streams.                                                                                                                                                                                                                                                                                                                                            |
| Backup Receiving Ports                | Backup Receiving Ports are used to define each port related to audio and video streams.                                                                                                                                                                                                                                                                                                                                     |
| <b>Outgoing Live Streams Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Unicast URL Reference                 | This field is auto-populated with a list of suggested URLs by using the Origin Server and the Service Routing Domain Name fields associated with the live delivery service. Choose one from the drop-down list.                                                                                                                                                                                                             |
| Enable Multicast Delivery to Client   | If enabled, the program uses multicast transmission.<br><br>If you wish to enable support for Content Acquirer failover, you must check this check box. Content Acquirer failover for a live program works only when the incoming stream is a multicast stream.                                                                                                                                                             |
| Multicast URL Reference               | This field is available if the <b>Enable Multicast Delivery to Client</b> check box is checked. The multicast URL reference (Announce URL) has the following format:<br><br>http://sourceHost_or_FQDN/path/filename.sdp<br><br>This URL uses the Origin Server and the Service Routing Domain Name and points to a meta-file (SDP) that is generated and resides on an external server. Choose one from the drop-down list. |
| Multicast TTL                         | Specify the multicast time-to-live (number of hops). The default is 15 hops.                                                                                                                                                                                                                                                                                                                                                |
| Multicast Address                     | The multicast address to use for streaming this program using multicast. The address range is 224.0.0.0 to 239.255.255.255. These values must be unique within the system.                                                                                                                                                                                                                                                  |
| Multicast Port                        | The multicast port to use for streaming this program using multicast. The port number must be even and within the range of 1 to 65535. These values must be unique within the system.<br><br>Even numbered ports are for Real-Time Transport Protocol (RTP), and odd numbered ports are for Real-Time Transport Control Protocol (RTCP).                                                                                    |

**Step 10** Click **Submit** to save the settings.

**Step 11** From the left-panel menu, choose **Schedule**. The Schedule page is displayed.

**Step 12** Click the **Play Forever** radio button to have the program play continuously.

Alternatively, click the **Schedule Playtime** radio button to schedule up to ten different playtimes. The Playtime Editor is displayed in the page.

To edit an existing playtime, click the **Edit** icon next to the Initial Start Time.

To delete an existing playtime, click the **Delete** icon next to the Initial Start Time.

**Step 13** Enter the settings for the playtime as appropriate. See [Table 8-11](#) for a description of the fields.

**Table 8-11 Playtime Fields**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start Playback on              | Start date and time for the program.                                                                                                                                                                                                                                                                                                                                  |
| UTC or SE (Local) Time         | Which clock the start time should use, UTC or SE local.                                                                                                                                                                                                                                                                                                               |
| Duration                       | Length of the program. In the drop-down list, choose minutes, hours, or days as the unit of time.                                                                                                                                                                                                                                                                     |
| Repeat Frequency               | The repeat frequency has the following options: <ul style="list-style-type: none"> <li>• Do Not Repeat—Plays once.</li> <li>• Repeat Every—Repeats every so many days, hours, or minutes.</li> <li>• Repeat Weekly—Repeats at the same hour on the days you choose.</li> </ul>                                                                                        |
| Repeat Forever<br>Repeat Until | These fields display when <b>Repeat Every</b> or <b>Repeat Weekly</b> are chosen for Repeat Frequency.<br><br>Repeat Forever repeats the program forever using the repeat frequency set in the previous fields.<br><br>Repeat Until repeats the program based on the repeat frequency set in the previous fields and until the date and time specified in this field. |

**Step 14** Click **Submit** to save the settings.

Click **Add Playtime** to add additional playtimes to an existing schedule. The Playtime Editor is displayed in the page.

## Priming a Live Delivery Service

The first client requesting a program often experiences the longest wait time for the program to begin playing. Users can experience long wait times because of the full RTSP negotiation that is required to pull the live stream from the source. Delays can also occur if the edge SE has not buffered enough stream data to fill the media player's buffer at the time the program is requested. For Windows Media streaming, when the buffer is not filled, some data to the client might be sent at the suboptimal line rate instead of at the Fast Start rate.

Delivery services for unicast-managed live programs can be primed for faster start-up times. When a live delivery service is primed, a unicast-out stream is pulled from the origin server to an SE before a client ever requests the stream. When the first request for the stream goes out, the stream is already in the delivery service.



### Note

It is not possible to monitor non-primed streams because they are played directly from the origin server. Primed streams can be monitored because they are buffered on the SE.



## Configuring a Rebroadcast

Once you have defined the program type for a rebroadcast program, you need to select media files, configure the streaming, and create a schedule. This procedure takes you through these steps and assumes you have already defined the program (see the “[Defining a Program](#)” section on page 8-26).



### Note

For rebroadcast programs, media can only be selected from one delivery service. The SEs and device groups assigned to the delivery service are selected automatically when you choose the media files for the program.

To configure a Movie Streamer rebroadcast or Windows Media rebroadcast program:

- Step 1** After you have chosen a program from the Program Table page, click **Select Media**. The Select Media page is displayed.
- Step 2** Choose a delivery service from the list by clicking the radio button next to the name of the delivery service and click **Show Media in Selected Delivery Service**. The Media File Selection pane is displayed.
- Step 3** In the **Criteria** field, enter the search criteria for the media files you want to add to the program and click **Use Criteria**. All the media files that match the search criteria are displayed.  
  
Use an asterisk (\*) to match any number of characters, or a question mark (?) to match exactly one character. For example, use “\*.mpg” for all files with the suffix “mpg,” and “file?.mpg” to match file1.mpg, file2.mpg, and so on.  
  
To start a new search, click **Select Media**.  
  
To choose a new delivery service to choose files from, click **All Delivery Services**, choose a delivery service, and click **Show Media in Selected Delivery Service**.
- Step 4** Check the **Pick** check box next to each file you want to rebroadcast and click **Add Media**. The files are displayed in the Media Files in Program pane.  
  
To select all files, click **All**. To deselect all files, click **None**. The file list can span several pages. To see the files from the other pages, click the page number, or from the **Row** drop-down list, select one of the options.
- Step 5** In the Media Files in Program pane, use the Up arrow and Down arrow next to each file to alter the order of the files. Files are played in the order in which they are listed.



### Note

The Up arrow and Down arrow are only displayed if the list of media files in the program is sorted by position. If you sort the media files by name or length, the arrows are not displayed.



### Note

Only one media file can be selected for Movie Streamer rebroadcasts.

To remove a media file from the list, check the **Pick** check box next to the file, and click **Remove Media**. To select all files, click **All**. To deselect all files, click **None**.

- Step 6** Click **Submit** to save the settings.

**Note**

For rebroadcast programs, media can only be selected from one delivery service. The SEs assigned to that delivery service are selected automatically when you choose the media files for the program. If at a later time you add new SEs to the delivery service, you must manually add them to the program.

**SE Assignment or Device Group Assignment**

[Step 7](#) through [Step 9](#) use the Assign Service Engines option to describe the procedure of assigning the Service Engines to the rebroadcast program. If you have device groups defined, you can use the Assign Device Groups option instead. To assign device groups, follow [Step 7](#) through [Step 9](#) and substitute Device Groups for each instance of SE.

- Step 7** To add new SEs to the rebroadcast program, from the left-panel menu, choose **Assign Service Engines**. The Service Engine Assignment page is displayed.
- Step 8** Click the **Assign** icon (blue X) next to the SE you want to assign to this delivery service. Or, in the task bar, click the **Assign All Service Engines** icon. The SE assignment states are described in [Figure 8-15](#).

**Figure 8-15 SE Assignment State**

|                                                                                    |                                                                                    |                                                                                    |                                                                                    |                                                                                            |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| New Assign                                                                         | Assigned and waiting for Submit                                                    | Assignment Submitted                                                               | Unassign Submitted Assignment                                                      | Not modifiable. The quota on all the delivery services for this SE exceeds the disk space. |
|  |  |  |  |        |

A green arrow wrapped around the blue X indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon.

- Step 9** Click **Submit** to save the SE assignments.
- A green circle with a check mark indicates an SE is assigned to this delivery service. To unassign the SE, click this icon, or click the **Unassign All Service Engines** icon in the task bar. Click **Submit** to save the changes.
- Step 10** From the left-panel menu, choose **Streaming**. The Streaming Settings page is displayed.
- Step 11** Enter the settings as appropriate. See [Table 8-12](#) for a description of the Windows Media Rebroadcast Stream Settings fields, and [Table 8-13](#) for a description of the Movie Streamer Rebroadcast Stream Settings fields.

**Table 8-12 Windows Media Rebroadcast Stream Settings Fields**

| Field                       | Description                                                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------|
| Multicast URL Reference     | The reference URL for multicast streaming has the following format: <code>http://SRDN/program-name.nsc</code> . |
| NSC Reference for Multicast | The URL for the NSC file used for a server-side playlist as the media source in a multicast program.            |

**Table 8-12 Windows Media Rebroadcast Stream Settings Fields (continued)**

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multicast Address and Port | <p>The multicast address and port to use for streaming this program using multicast. The address range is 224.0.0.0 to 239.255.255.255.</p> <p>The port number must be even and within the range of 1 to 65535. These values must be unique within the system.</p> <p>Even numbered ports are for Real-Time Transport Protocol (RTP), and odd numbered ports are for Real-Time Transport Control Protocol (RTCP).</p> |
| Multicast TTL              | Specify the multicast time-to-live (number of hops). The default is 15 hops.                                                                                                                                                                                                                                                                                                                                          |

**Table 8-13 Movie Streamer Rebroadcast Stream Settings Fields**

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multicast URL Reference    | The reference URL for multicast streaming has the following format: <code>http://SRDN/programID.sdp</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Multicast TTL              | Specify the multicast time-to-live (number of hops). The default is 15 hops.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Multicast Address and Port | <p>The multicast address and port to use for streaming this program using multicast. The address range is 224.0.0.0 to 239.255.255.255.</p> <p>The port number must be even and within the range of 1 to 65535. These values must be unique within the system.</p> <p>Even numbered ports are for Real-Time Transport Protocol (RTP), and odd numbered ports are for Real-Time Transport Control Protocol (RTCP).</p> <p><b>Note</b> Because Movie Streamer rebroadcast files can contain multiple tracks (1 to 3), you can define up to three multicast addresses and ports for each track in the file. Click <b>Add Multicast Address/Port</b> to add another multicast address.</p> |

**Step 12** Click **Submit** to save the settings.

**Step 13** From the left-panel menu, choose **Schedule**. The Schedule page is displayed.

**Step 14** Click the **Loop Back Continuously** radio button to have the program play continuously.

Alternatively, click the **Schedule Playback** radio button to schedule up to ten different playback times. The Playtime Editor is displayed in the page.

To edit an existing playtime, click the **Edit** icon next to the Initial Start Time.

To delete an existing playtime, click the **Delete** icon next to the Initial Start Time.

**Step 15** Enter the settings for the playtime as appropriate. See [Table 8-14](#) for a description of the fields.

**Table 8-14**      **Playtime Fields**

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start Playback on              | The start date and time for the program.                                                                                                                                                                                                                                                                                                                              |
| UTC or SE (Local) Time         | Which clock the start time should use, UTC or SE local.                                                                                                                                                                                                                                                                                                               |
| Duration                       | The length of the program. In the drop-down list, choose minutes, hours, or days as the unit of time.                                                                                                                                                                                                                                                                 |
| Playback Options               | The playback options are the following: <ul style="list-style-type: none"> <li>• Playback Once and Stop</li> <li>• Loop for number of minutes, hours, or days</li> </ul>                                                                                                                                                                                              |
| Repeat Frequency               | The repeat frequency has the following options: <ul style="list-style-type: none"> <li>• Do Not Repeat—Plays once.</li> <li>• Repeat Every—Repeats every so many days, hours, or minutes.</li> <li>• Repeat Weekly—Repeats at the same hour on the days you choose.</li> </ul>                                                                                        |
| Repeat Forever<br>Repeat Until | These fields display when <b>Repeat Every</b> or <b>Repeat Weekly</b> are chosen for Repeat Frequency.<br><br>Repeat Forever repeats the program forever using the repeat frequency set in the previous fields.<br><br>Repeat Until repeats the program based on the repeat frequency set in the previous fields and until the date and time specified in this field. |

**Step 16** Click **Submit** to save the settings.

Click **Add Playtime** to add additional playtimes to an existing schedule. The Playtime Editor is displayed in the page.

## Viewing the Multicast Addresses

The multicast delivery feature is enabled by setting up a multicast address for a live or rebroadcast program to which different client devices, configured to receive content from the same program, can subscribe. The delivering device sends content to the multicast address set up at the delivery service, from which it becomes available to all subscribed receiving devices.

A set of multicast addresses can be specified either in the Program API or by using the CDSM. When a program requires a multicast address, you can specify the multicast address within the stream settings of the program. Addresses are allocated for the life of a program.

To view the multicast addresses used by live programs and rebroadcasts, choose **Services > Live Video > Multicast Addresses**. The Multicast Addresses page is displayed.

The list of multicast addresses that have been currently configured for specific programs is displayed in the Multicast Addresses table.

# Viewing Programs

The Programs Table page lists all the programs defined in your ECDS network. Programs can be defined through the CDSM or through an API. For information on adding or editing a program definition, see the [“Defining a Program” section on page 8-26](#).

The Programs Table page allows you to view scheduled programs by day, week, month, or year. You can sort and filter programs by name, type, or schedule. You can also preview live programs while they are playing. See the [“Previewing a Program” section on page 8-39](#) for more information.

[Table 8-15](#) describes the icons for the Programs Table page.

**Table 8-15 Programs Table Icons**

| Icon                                                                                | Function                                                                                                      |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|    | Creates a new program. See the <a href="#">“Defining a Program” section on page 8-26</a> for more information |
|    | Creates a filtered table. Filter the table based on the field values.                                         |
|    | Views all table entries. Click this icon to view all entries after you have created a filtered table.         |
|   | Refreshes the table.                                                                                          |
|  | Prints the current window.                                                                                    |
|  | Edits a program. See the <a href="#">“Defining a Program” section on page 8-26</a> for more information       |

To view all the programs defined in your ECDS network:

- Step 1** Choose **Services > Live Video > Live Programs**. The Programs Table page displays with a list of all the programs that have been defined through either the CDSM or the Program API.
- Step 2** Click the **Day**, **Week**, **Month**, or **Year** tab to view the playback schedules. Scheduled programs are listed by start time (initial start time plus any repeat intervals). Times begin with the current device time (current system time plus device time zone offset).  
  
The **Unscheduled** tab displays all unscheduled programs defined in your ECDS network. The **All** tab displays all the programs defined in your ECDS network. The Programs Table page opens to the All view by default.
- Step 3** Sort columns by clicking the column heading. You can also combine filtering conditions. For example, you can filter only Windows Media live programs and then choose the **Week** tab to view the week of November 23 to November 29, 2007. [Table 8-16](#) describes the information that is displayed in this page.

**Table 8-16**      **Programs Table Page Information**

| Item                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tabs</b>                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Day/Week/Month/Year          | Lists programs based on their schedule. The current day, week, month, or year is displayed by default. You can navigate to the next or previous day, week, month, or year by clicking the back or forward arrows on either side of the date.                                                                                                                                                                                                                                                                                   |
| Unscheduled                  | Lists only programs with no schedule defined.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| All                          | Lists all programs. This is the default view.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Program Listing Table</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Program                      | Program name, which must be unique to the CDSM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Type                         | Program type. Program types are: <ul style="list-style-type: none"> <li>• Movie Streamer live</li> <li>• Movie Streamer rebroadcast</li> <li>• Windows Media live</li> <li>• Windows Media rebroadcast</li> </ul>                                                                                                                                                                                                                                                                                                              |
| Schedule                     | Describes the schedule. Options are: <ul style="list-style-type: none"> <li>• None (the program has no schedule)</li> <li>• Loop continuously</li> <li>• Number of playtimes (the number of times that the program is scheduled to be shown)</li> </ul> Start Time—Program start time in a scheduled view (Day, Week, Month, or Year tab). Lists up to three start times if repeat broadcasts are configured.<br><br>Duration—Duration of the program or the looping time in a scheduled view (Day, Week, Month, or Year tab). |

## Viewing and Modifying API Programs

Programs created through APIs are based on a program file. A *program file* contains the elements that define the schedule, content, and presentation parameters. It is a text file written in XML format, similar to the Manifest file. The program file contains most of the program settings and resides on an external server. The CDSM gets the program file, parses it, and saves the program file to the database. The program is automatically updated at intervals by the CDSM refetching the program file and reparsing it. The program file supports RTSP.

In contrast, programs defined using the CDSM are not based on a program file; instead, the settings entered in the CDSM are saved directly to the database.

Programs created using an API can be viewed in the CDSM as read-only, and modifications to API programs can be done through the API. You can also edit the API program using the CDSM; however, if you choose this option, the information about the API program file is deleted and the program can no

longer be modified through the API. A third option is to copy the API program using the CDSM Copy Program feature. The new copy does not contain the program file information and is treated as a CDSM-generated program for the purposes of editing. (See the “[Copying a Program](#)” section on [page 8-39](#).)

You can delete any program from the list (whether created through the CDSM or through an API) in the Programs Table page.

## Previewing a Program

You can preview live programs by live split or by joining a multicast broadcast. Live programs can only be viewed during the scheduled playtime. You can preview a rebroadcast program by joining the multicast broadcast during the scheduled playtime.

To preview a live Movie Streamer or Windows Media program or scheduled rebroadcast:

- 
- Step 1** Choose **Services > Live Video > Live Programs**. The Programs Table page is displayed.
  - Step 2** Click the **Day, Week, Month, or Year** tab.
  - Step 3** Click the **Play** icon next to the name of a program. A program preview window pops up, displaying the program information with links to view the program.




---

**Note** The **Play** icon only appears while the live program is playing. If a program is not currently playing, you cannot view it.

---

- Step 4** Click the URL reference link for the program. You have the option to choose a multicast or unicast URL reference, if such are defined for the program. A new window with the URL reference opens.
- 

To successfully view the program, you must meet these conditions:

- You must be able to access the client network.
- Windows Media plug-in installed to view Windows Media live programs.
- QuickTime plug-in installed to view Movie Streamer live programs.

## Copying a Program

The copy program feature allows you to create a copy of an existing program and then modify a subset of attributes, which eliminates the need to re-enter all the program settings each time you create programs with similar characteristics.

When you copy a program, a duplicate of the program is created and saved to the database. Any changes that you make to the new copy of the program do not affect the original program and vice versa. Note, however, that if multicast is configured, the multicast address and port cannot be copied. These parameters must be unique across the system. If a program address pool is configured, these parameters can be automatically selected by the system.

To create a copy of an existing program:

- 
- Step 1** Choose **Services > Live Video > Live Programs**. The Programs Table page is displayed.

- Step 2** Click the **Edit** icon next to the name of the program that you want to copy. The Program Definition page is displayed.
- Step 3** Click the **Copy Program** icon in the task bar. You are prompted to confirm your decision. Click **OK**. The window refreshes, displaying ProgramName\_dup in the Name field.
- Step 4** Edit any program information that you want to change. (See the “[Defining a Program](#)” section on [page 8-26](#).)
-  **Note** You cannot change the program type.
- Step 5** Click **Submit** to save the settings.
- Step 6** Edit any of the other program properties found in the left-panel menu, such as the program schedule, program, or device assignments.
- 

## Where to Go Next

Proceed to [Chapter 9, “Configuring the System”](#) for information about configuring ECDS system parameters.

**Tip**

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Configuration Guide on Cisco.com.

---





## CHAPTER 9

# Configuring the System

---

The following sections describe how to configure ECDS system parameters:

- [Configuring AAA, page 9-1](#)
- [Changing a Password, page 9-6](#)
- [Configuring System Settings, page 9-7](#)
- [Where to Go Next, page 9-14](#)

## Configuring AAA

*Authentication* determines who the user is and whether that user should be allowed access to the network or a particular device. It allows network administrators to bar intruders from their networks. It may use a simple database of users and passwords. It can also use one-time passwords.

*Authorization* determines what the user is allowed to do. It allows network managers to limit which network services are available to different users.

*Accounting* tracks what users did and when they did it. It can be used for an audit trail or for billing for connection time or resources used (bytes transferred).

Collectively, authentication, authorization, and accounting are sometimes referred to as AAA. Central management of AAA means the information is in a single, centralized, secure database, which is much easier to administer than information distributed across numerous devices.

In the ECDS network, login authentication and authorization are used to control user access and configuration rights to the CDSM, SEs, and SRs. There are two levels of login authentication and authorization:

- Device
- CDSM

In an ECDS network, user accounts can be created for access to the CDSM and, independently, for access to the SEs and SRs that are registered to the CDSM.

This section covers login authentication and authorization for the CDSM. For information about device login authentication and authorization, see the [“Login Access Control” section on page 5-65](#) and the [“Authentication” section on page 5-71](#).

Login authentication is the process by which CDSM verifies whether the person who is attempting to log in has a valid username and password. The person logging in must have a user account registered with the device. User account information serves to authorize the user for login and configuration

privileges. The user account information is stored in the AAA database. When the user attempts to log in, the CDSM compares the person's username, password, and privilege level to the user account information that is stored in the database.

Each user account can be assigned to a role and a domain. A *role* defines which CDSM configuration pages the user can access and which services the user has authority to configure or modify. A *domain* defines which entities in the network the user can access and configure or modify. You can assign a user account to zero or more roles, and to zero or more domains.

## Creating, Editing, and Deleting Users



### Note

This section is addressed to users with administrator-level privileges (admin users) only.

Two default user accounts are preconfigured in the CDSM. The first account, called *admin*, is assigned the administrator role that allows access to all services and access to all entities in the system. This account cannot be deleted from the system, but it can be modified. Only the username and the role for this account are unchangeable. To change the password for this account, use the **username admin password <password>** command through the CLI.

The second preconfigured user account is called *default*. Any user account that is authenticated but has not been registered in the CDSM gets the access rights (role and domains) assigned to the default account. This account is configurable, but it cannot be deleted nor can its username be changed.

When you create a new user account in the CDSM, you have the option to create the user account in the CLI for the CDSM device at the same time. Using this option to create the new account in the CLI provides the following benefits:

- User account is created in the primary and standby CDSM management databases and in the CDSM CLI from one central point.
- Users can change their passwords, and the password changes are propagated to a standby CDSM.

If you choose to create the user account from the CDSM *without* creating the user account in the CDSM CLI at the same time, the following results apply:

- User account is created in the primary and standby CDSM management databases.
- No user account is created in the CDSM CLI, and the user *cannot* log in to the CDSM until an account is created from the CLI.
- Local users cannot change their passwords using the CDSM.
- Local users can change their passwords using the CLI; however, the password changes are not propagated from the CLI to the CDSM databases when the CLI user option is enabled in the CDSM.

If a user account has been created from the CLI only, when you log in to the CDSM for the first time, the Centralized Management System (CMS) database automatically creates a user account (with the same username as configured in the CLI) with default authorization and access control. However, to change the password in this scenario, the user account must be explicitly configured from the CDSM with the CLI user option enabled.

To create or edit a user account:

**Step 1** Choose **System > AAA > Users**. The User Table page is displayed.

[Table 9-1](#) describes the icons for the User Table page.

**Table 9-1 User Table Icons**

| Icon                                                                              | Function                                                                                              |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
|  | Creates a new entry.                                                                                  |
|  | Edits an entry.                                                                                       |
|  | Creates a filtered table. Filter the table based on the field values.                                 |
|  | Views all table entries. Click this icon to view all entries after you have created a filtered table. |
|  | Refreshes the table.                                                                                  |
|  | Prints the current window.                                                                            |

**Step 2** Click the **Create New** icon in the task bar. The User Account page is displayed.

To edit an account, click the **Edit** icon next to the username.



**Note** The User Account page can only be accessed by users with administrator-level privileges.

**Step 3** In the **Username** field, enter the user account name. The username must be between 4 and 32 characters in length, and begin with a letter.

**Step 4** If you want to create a local user account with a password and privilege level from the CDSM, check the **Create CLI User** check box. The user account is created automatically in the CLI. To prevent the creation of a CLI user account from the GUI, leave the check box unchecked.

**Step 5** In the **Password** field, enter a password for the CLI user account, and re-enter the same password in the **Confirm Password** field.

The password strength must be a combination of alphabetic character, at least one number, at least one special character, and at least one uppercase character.

**Step 6** From the Privilege Level drop-down list, choose a privilege level for the CLI user account. The choices are 0 (zero) (normal user) or 15 (superuser). The default value is 0.



**Note** A superuser can use privileged-level EXEC commands, whereas a normal user can use only user-level EXEC commands.

**Step 7** In the Username Information area, enter the following information about the user: First Name, Last Name, Phone Number, Email Address, Job Title, and Department.

**Step 8** In the **Comments** field, enter any additional information about this account.

**Step 9** Click **Submit** to save the settings.

**Step 10** From the left-panel menu, click **Role Management**. The Role Management Table page is displayed.

[Table 9-1](#) describes the icons for the Role Management page.

**Table 9-2 Role Management Icons**

| Icon                                                                                | Function                                                                                              |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
|    | Creates a new entry.                                                                                  |
|    | Edits an entry.                                                                                       |
|    | Creates a filtered table. Filter the table based on the field values.                                 |
|    | Views all table entries. Click this icon to view all entries after you have created a filtered table. |
|    | Refreshes the table.                                                                                  |
|    | Assigns all roles.                                                                                    |
|    | Removes all roles.                                                                                    |
|    | Views read-only items.                                                                                |
|  | Indicates that the current transaction was successfully completed.                                    |

To add roles, see the [“Creating, Editing, and Deleting Roles”](#) section on page 9-5.

To view the setting for the role, click the **View** (eyeglasses) icon next to the role.

- Step 11** Click the **Assign** icon (blue cross mark) next to each role name you want to assign to the user account. To remove the role from the user account, click the **Assign** icon again.

To assign all roles, click the **Assign all Roles** icon in the task bar. To unassign all roles, click the **Remove all Roles** icon in the task bar.

- Step 12** Click **Submit** to save the settings.

A green arrow wrapped around the blue cross mark indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon.

- Step 13** From the left-panel menu, click **Domain Management**. The Domain Management Table page is displayed.

To add domains, see the [“Creating, Editing, and Deleting Domains”](#) section on page 9-6.

To view the setting for the domain, click the **View** (eyeglasses) icon next to the domain.

- Step 14** Click the **Assign** icon next to each domain name you want to assign to the user account.

To remove the domain from the user account, click the **Assign** icon again.

To assign all domains, click the **Assign All** icon in the task bar. To unassign all domains, click the **Remove All** icon in the task bar.

**Step 15** Click **Submit** to save the settings.

To delete a user, in the User Table page, click the **Edit** icon next to the username, and from the User Account page, click the **Delete** icon in the task bar.



**Note**

Deleting a user account from the CLI does *not* delete the corresponding account in the CDSM database. User accounts created in the CDSM should always be deleted from within the CDSM.

## Creating, Editing, and Deleting Roles

Although the CDSM provides many types of services, not all users have access to all services. Users are assigned a role, which indicates the services to which they have access. A *role* is a set of enabled services.

Each user account can be assigned zero or more roles. Roles are not inherited or embedded. The CDSM provides one predefined role, known as the *admin role*. The admin role has access to all services and all ECDS network entities.



**Note**

The admin user account, by default, is assigned to the role that allows access to all domains and all entities in the system. It is not possible to change the role for this user account.

To create or edit a role:

- 
- Step 1** Choose **System > AAA > Roles**. The Roles Table page is displayed.
  - Step 2** Click the **Create New** icon in the task bar. The Role page is displayed.  
To edit a role, click the **Edit** icon next to the role name.
  - Step 3** In the **Name** field, enter the name of the role.
  - Step 4** To enable read-only access for this role, check the **Read-Only** check box. Users assigned to this role are only be able to view the CDSM pages. They are not able to make any changes.
  - Step 5** To expand a listing of services under a category, click the folder, and then check the check box next to the service or services you want to enable for this role. To choose all the services under one category simultaneously, check the check box for the top-level folder.
  - Step 6** In the **Comments** field, enter any comments about this role.
  - Step 7** Click **Submit** to save the settings.
- 

To delete a role, in the Roles Table page, click the **Edit** icon next to the role name. Once the Role page is displayed, click the **Delete** icon in the task bar.

## Creating, Editing, and Deleting Domains

A *domain* is a set of ECDS network entities or objects that make up the ECDS network. Whereas a role defines which services a user can perform in the ECDS network, a domain defines the entities to which the user has access. An *entity* can be a Service Engine, a device group, or a delivery service. These predefined entities are treated like services and can be enabled or disabled when you set up user roles.

When you configure a domain, you can choose to include Service Engines, device groups, or delivery services in the domain.

To create or edit a domain:

- 
- Step 1** Choose **System > AAA > Domains**. The Domains Table page is displayed.
  - Step 2** Click the **Create New** icon in the task bar. The Domain page is displayed.  
To edit a domain, click the **Edit** icon next to the domain name.
  - Step 3** In the **Name** field, enter the name of the domain.
  - Step 4** From the **Entity Type** drop-down list, choose Service Engines, Device Groups, or Delivery Services.
  - Step 5** In the **Comments** field, enter any comments about this domain.
  - Step 6** Click **Submit** to save the settings. If the entity type you chose has not already been assigned to the domain, then a message displays indicating that the entity type has not been assigned.
  - Step 7** From the left-panel menu, click **Entity Management**. The Entity Management page is displayed.
  - Step 8** Click the **Assign** icon (blue cross mark) next to each entity name you want to include. A green arrow wrapped around the blue cross mark indicates an entity is assigned.  
To assign all entities in the domain, click the **Assign All** icon in the task bar.  
To remove an entity from the domain, click the **Assign** icon again.  
To remove all entities from the domain, click the **Remove All** icon in the task bar.
  - Step 9** Click **Submit** to save the settings.
- 

To delete a domain, in the Domain Table page click the **Edit** icon next to the domain name. Once the Domain page is displayed, click the **Delete** icon in the task bar.

## Changing a Password

If you are a user *without* admin privileges and you are logged in to the CDSM, you can change your own CDSM and CLI user password if you meet the following requirements:

- Your CLI user account and password were created in the CDSM and not in the CLI.
- You are authorized to access the Password page.



### Caution

We do not recommend changing the CLI user password from the CLI. Any changes to CLI user passwords from the CLI are *not* updated in the management database and are not propagated to the standby CDSM. Therefore, passwords in the management database do not match a new password

configured in the CLI.

The advantage of initially setting passwords from the CDSM is that both the primary and the standby CDSMs are synchronized, and CDSM users do not have to access the CLI to change their passwords.

To change the CDSM and CLI user password for the user account that is currently logged in to the CDSM:

- 
- Step 1** Choose **System > Password**. The Password page is displayed.
- Step 2** In the **New Password** field, enter the changed password.
- Step 3** In the **Confirm New Password** field, re-enter the password for confirmation.
- Step 4** Click **Submit** to save the settings.
- 

## Configuring System Settings

This section covers the following topics:

- [System Properties, page 9-7](#)
- [Configuring Fast SE Offline Detection, page 9-8](#)
- [Configuring Distribution QoS, page 9-10](#)
- [Configuring Service Routing, page 9-11](#)

## System Properties

To modify the system properties:

- 
- Step 1** Choose **System > Configuration > System Properties**. The System Properties page is displayed.
- Step 2** Click the **Edit** icon next to the system property you want to change. The Modify Config Property page is displayed.
- Step 3** For true or false values, choose a setting from the **Value** drop-down list. For other values, enter a new value. The range is displayed for each numeric value.

[Table 9-3](#) describes the system properties.

**Table 9-3**      **System Properties Fields**

| Field                              | Description                                                                                                                            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| cdsm.session.timeout               | Length of a Content Distribution Manager session (in minutes). The default is 10. The range is from 5 to 120.                          |
| DeviceGroup.overlap                | SE feature overlapping (true or false).                                                                                                |
| System.CmsUnsProgram Sync.Interval | Interval by which CMS synchronizes program import UNS objects (in minutes). The default is 1440 minutes. The range is from 1 to 43200. |
| System.datafeed.pollRate           | Poll rate between the SE or the SR and the CDSM (in seconds). The default is 300. The range is from 30 to 1800.                        |

**Table 9-3**      **System Properties Fields (continued)**

| Field                                            | Description                                                                                                                                                                                           |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System.device.recovery.key                       | Device identity recovery key. This property enables a device to be replaced by another node in the ECDS network.                                                                                      |
| System.healthmonitor.collect Rate                | Sets the collect and send rate in seconds for the CMS device health (or status) monitor. The default is 120. The range is from 5 to 3600.                                                             |
| System.Icm.enable                                | Local and CDSM feature (true or false). This property allows settings that are configured using the local device CLI or the CDSM to be stored as part of the ECDS network configuration data.         |
| System.monitoring.collect Rate                   | Rate at which the SE collects and sends the monitoring report to the CDSM (in seconds). The default is 300 seconds. The range is from 30 to 1800.                                                     |
| System.monitoring.daily ConsolidationHour        | Hour at which the CDSM consolidates hourly and daily monitoring records. The default is 1. The range is from 0 to 23.                                                                                 |
| System.monitoring.enable                         | SE statistics monitoring (true or false).                                                                                                                                                             |
| System.monitoring.monthly ConsolidationFrequency | Frequency (in days) with which the CDSM consolidates daily monitoring records into monthly records. The default is 14. The range is from 1 to 30.                                                     |
| System.monitoring.record LimitDays               | Maximum number of days of monitoring data to maintain in the system. The default is 1825. The range is from 0 to 7300.                                                                                |
| System.repstatus.update Enabled                  | Replication status periodic calculations on an SE (enable or disable).                                                                                                                                |
| System.repstatus.updateRate                      | Rate of replication status periodic updates calculated on an SE (in minutes). The default is 10. The range is from 5 to 1440.                                                                         |
| System.repstatus.updateRate Sec                  | Rate of replication status periodic updates calculated on an SE (in seconds). The default is 600 seconds. Setting this rate overrides the update rate set in minutes. The ranges is from 30 to 86400. |
| System.repstatus.updateSync Enabled              | Sending summary replication status with requested detailed status (true or false).                                                                                                                    |

**Step 4** Click **Submit** to save the settings.

## Configuring Fast SE Offline Detection

You can detect offline SEs more quickly if you enable the Fast Detection of Offline SEs feature.

If Fast Detection of Offline SEs is not enabled, the CDSM waits for at least two “System.datafeed.pollRate” polling periods before declaring the SE offline.

If Fast Detection of Offline SEs is enabled, the CDSM waits until the value displayed in the Maximum Offline Detection Time field, located on the Configure Fast SE Offline Detection page, is exceeded.

Communication between the SE and CDSM using User Datagram Protocol (UDP) allows faster detection of SEs that have gone offline. UDP heartbeat packets are sent at a specified interval from each SE to the primary CDSM in an ECDS network. The primary CDSM tracks the last time it received a UDP heartbeat packet from each SE. If the CDSM has not received the specified number of UDP packets, it



displays the status of the nonresponsive SEs as offline. Because UDP heartbeats require less processing than a getUpdate request, they can be transmitted more frequently, and the CDSM can detect offline SEs much faster.

An SE is declared offline when it has failed to contact the CDSM for a getUpdate request (get configuration poll) for at least two polling periods.

**Note**

In ECDS networks with heavy traffic, dropped UDP packets can cause the CDSM to incorrectly report the status of SEs as offline. To avoid this problem, configure a higher value for dropped UDP heartbeat packets.

To configure Fast Detection of Offline SEs:

- Step 1** Choose **System > Configuration > Fast SE Offline Detection**. The Configure Fast SE Offline Detection page is displayed.

**Note**

The Fast Detection of Offline SEs feature is in effect only when the CDSM receives the first UDP heartbeat packet and a getUpdate request from an SE.

- Step 2** Check the **Enable** check box to enable the CDSM to detect the offline status of SEs quickly.

**Note**

SEs can have their software upgraded without any errors in the status being displayed in the CDSM if you disable Fast Detection of Offline SEs.

- Step 3** In the **Heartbeat Rate** field, specify how often, in seconds, the SEs should transmit a UDP heartbeat packet to the CDSM. The default is 30. The range is from 30 to 3600.

- Step 4** In the **Heartbeat Fail Count** field, specify the number of UDP heartbeat packets that can be dropped during transmission from SEs to the CDSM before an SE is declared offline. The default is 1. The range is from 1 to 100.

- Step 5** In the **Heartbeat UDP Port** field, specify the CDSM port number that the SEs use to send UDP heartbeat packets. The default is 2000. The range is from 1000 to 10000.

The **Maximum Offline Detection Time** field displays the product of the failed heartbeat count and heartbeat rate, where:

$$\text{Maximum Offline Detection Time} = \text{Failed heartbeat count} * \text{Heartbeat rate}$$

If Fast Detection of Offline SEs is enabled, the CDSM detects SEs that are in network segments that do not support UDP and uses a getUpdate request (get configuration poll) to detect offline SEs.

If the CDSM does not receive regular keep-alive communication from an SE, the CDSM displays the SE as offline after a time period of  $2 * (\text{Heartbeat rate}) * (\text{Failed heartbeat count})$ .

- Step 6** Click **Submit** to save the settings.

## Configuring Distribution QoS

The Distribution QoS settings allow you to configure system-wide QoS priorities for delivery service distribution and metadata replication. The delivery service distribution priority (low, medium, or high) is set on the definition page for each delivery service.



### Note

When a single URL is associated with more than one delivery service, the content is distributed only one time to all the Service Engines subscribed to each delivery service. When different QoS settings are configured for different delivery services that contain the same content, the delivery service priority setting determines which QoS settings are applied to the content distribution. The delivery service with the higher priority dictates which QoS settings are used.

To configure system-wide QoS settings:

- Step 1** Choose **System > Configuration > Distribution QoS**. The Distribution QoS page is displayed.
  - Step 2** Check the **Set QoS for Unicast Data** check box to enable system-wide QoS settings for unicast data.  
The unicast data refers to the ingest and distribution traffic among SEs.
  - Step 3** To set the QoS value for a delivery service with low priority, choose a Differentiated Service Code Point (SCDP) value from the **QoS value with low priority** drop-down list. Alternatively, enter a decimal value in the corresponding field.
- 

**Note** See the next section, “[Setting DSCP Values for QoS Packets](#),” for more information. You can override the system-wide settings for unicast data by configuring QoS settings on a per-delivery service basis. See the “[Creating Delivery Service](#)” section on page 8-4 for more information.
- Step 4** To set the QoS value for a delivery service with medium priority, choose a DSCP value from the **QoS value with medium priority** drop-down list. Alternatively, enter a decimal value in the corresponding field.
  - Step 5** To set the QoS value for a delivery service with high priority, choose a DSCP value from the **QoS value with high priority** drop-down list. Alternatively, enter a decimal value in the corresponding field.
  - Step 6** Set the QoS value for each priority (low, medium, and high) for a delivery service by choosing the Differentiated Service Code Point (DSCP) value from the QoS value drop-down list or by entering a decimal value in the corresponding field.
  - Step 7** Check the **Set QoS for metadata** check box to enable QoS settings for metadata replication.  
Metadata is created based on the Manifest file and is part of the ingest and distribution traffic.
  - Step 8** Set the **QoS value for metadata replication** by choosing the DSCP value from the QoS value drop-down list or by entering a decimal value in the corresponding field.
  - Step 9** Click **Submit** to save the settings.

### Setting DSCP Values for QoS Packets

The ECDS allows you to set Differentiated Services Code Point (DSCP) values for Unicast QoS packets. DSCP values define relative priority levels for the packets. You can either choose a DSCP keyword from the drop-down list or enter a value in the corresponding field. (See [Table 9-4](#).)

**Table 9-4 DSCP Values**

| Keyword | Description and Value                                                                                                                    |
|---------|------------------------------------------------------------------------------------------------------------------------------------------|
| af11    | Sets packets with AF11 DSCP (001010).<br><b>Note</b> The number in parentheses denotes the DSCP value for each per-hop behavior keyword. |
| af12    | Sets packets with AF12 DSCP (001100).                                                                                                    |
| af13    | Sets packets with AF13 DSCP (001110).                                                                                                    |
| af21    | Sets packets with AF21 DSCP (010010).                                                                                                    |
| af22    | Sets packets with AF22 DSCP (010100).                                                                                                    |
| af23    | Sets packets with AF23 DSCP (010110).                                                                                                    |
| af31    | Sets packets with AF31 DSCP (011010).                                                                                                    |
| af32    | Sets packets with AF32 DSCP (011100).                                                                                                    |
| af33    | Sets packets with AF33 DSCP (011110).                                                                                                    |
| af41    | Sets packets with AF41 DSCP (100010).                                                                                                    |
| af42    | Sets packets with AF42 DSCP (100100).                                                                                                    |
| af43    | Sets packets with AF43 DSCP (100110).                                                                                                    |
| cs1     | Sets packets with CS1 (precedence 1) DSCP (001000).                                                                                      |
| cs2     | Sets packets with CS2 (precedence 2) DSCP (010000).                                                                                      |
| cs3     | Sets packets with CS3 (precedence 3) DSCP (011000).                                                                                      |
| cs4     | Sets packets with CS4 (precedence 4) DSCP (100000).                                                                                      |
| cs5     | Sets packets with CS5 (precedence 5) DSCP (101000).                                                                                      |
| cs6     | Sets packets with CS6 (precedence 6) DSCP (110000).                                                                                      |
| cs7     | Sets packets with CS7 (precedence 7) DSCP (111000).                                                                                      |
| default | Sets packets with the default DSCP (000000).                                                                                             |
| ef      | Sets packets with EF DSCP (101110).                                                                                                      |

## Configuring Service Routing

The Service Routing menu options consist of the following:

- [Coverage Zone File Registration, page 9-11](#)
- [Configuring Global Routing, page 9-13](#)

### Coverage Zone File Registration

A coverage zone can be associated with one or more SEs: each SE can have its own unique coverage zone, or SEs can be associated with more than one coverage zone and have overlapping coverage zones. For more information about coverage zones, see the following sections in this guide:

- [“Coverage Zone File”](#)
- [“Creating Coverage Zone Files”](#)

The system administrator places a Coverage Zone file where the CDSM or individual devices can access the URL. The administrator then registers the Coverage Zone file URL in the CDSM. Coverage Zone files can be applied globally to the entire ECDS network, or locally to a specific SR. If a Coverage Zone file is made global, then it is read and parsed by each SR that does not have a Coverage Zone file assigned. If the coverage zone is specified in an individual SR configuration, it is only applied to that particular SR.

You have the choice of using two types of coverage zones:

- Default coverage zones
- User-defined coverage zones

A default coverage zone consists of all the SEs that reside in the same local network segment, or subnet. The CDSM provides a check box to specify whether the default coverage zone is to be used.

A user-defined coverage zone consists of all the SEs that are specified in a Coverage Zone file. This file defines the network segments to be covered in the routing process. The Coverage Zone file is registered with the CDSM and then applied to an SR for routing definitions.

To apply a custom coverage zone to an SR, you first need to register a Coverage Zone file URL in the CDSM. After you have registered the Coverage Zone file URL with the CDSM, you can apply the Coverage Zone file in one of two ways:

- Globally—Deploy the Coverage Zone file across the entire ECDS network
- Locally—Deploy the Coverage Zone file on a specific SR


**Note**

If you apply a Coverage Zone file locally for a device, this file overwrites the global Coverage Zone file for that device.

To register a Coverage Zone file:

- Step 1** Choose **System > Configuration > Service Routing > Coverage Zone File Registration**. The Coverage Zone File Table page is displayed.
- Step 2** Click the **Create New** icon in the task bar. The Registering Coverage Zone File page is displayed.  
To edit a Coverage Zone file registration, click the **Edit** icon next to the registration you want to edit.
- Step 3** Choose a file import method from the **File Import Method** drop-down list:
  - **Upload**—The upload method allows you to upload a Coverage Zone file from any location that is accessible from your PC by using the browse feature.
  - **Import**—The import method allows you to import the Coverage Zone file from an external HTTP, HTTPS, FTP, or CIFS server.

When you choose a method, the page refreshes and displays the configuration fields that are associated with the method that you chose.
- Step 4** Enter the fields as appropriate. [Table 9-5](#) describes the upload method fields. [Table 9-6](#) describes the import method fields.

**Table 9-5 Upload Method for Coverage Zone Files**

| Property                  | Description                                                                                                                                                            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Coverage Zone File Upload | Local directory path to the Coverage Zone file. To locate the file, use the <b>Browse</b> button. Click the <b>Validate</b> button to validate the Coverage Zone file. |
| Destination Filename      | Name of the Coverage Zone file. This field is filled in automatically with the filename from the local directory path.                                                 |

**Table 9-6 Import Method for Coverage Zone Files**

| Property                     | Description                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Coverage Zone File URL       | The URL where the Coverage Zone file is located, including path and filename. Click the <b>Validate</b> button to validate the Coverage Zone file.                                                                                                                                                                                                                                     |
| Destination File Name        | Name of the Coverage Zone file.                                                                                                                                                                                                                                                                                                                                                        |
| Update Interval (minutes)    | Frequency with which the CDSM looks for changes to the Coverage Zone file. The default value is 10 minutes.                                                                                                                                                                                                                                                                            |
| Username                     | Name of the user to be authenticated when fetching the Coverage Zone file.                                                                                                                                                                                                                                                                                                             |
| Password                     | User password for fetching the Coverage Zone file.                                                                                                                                                                                                                                                                                                                                     |
| NTLM user Domain             | NT LAN Manager (NTLM) user domain name for NTLM authentication.                                                                                                                                                                                                                                                                                                                        |
| Disable Basic Authentication | When checked, NTLM headers cannot be stripped off to allow fallback to the basic authentication method.<br><br>If you leave this check box unchecked, NTLM authentication headers can be stripped to allow fallback to the basic authentication method, and the username and password information can be passed to the origin server in clear text with a basic authentication header. |

**Step 5** To save the settings, click **Submit**.

## Configuring Global Routing

After you have registered the Coverage Zone file, you can use this file as your global routing configuration.

To set a global Coverage Zone file:

- Step 1** Choose **System > Configuration > Service Routing > Global Routing Config**. The Set Global Coverage Zone File page is displayed.
- Step 2** From the **Coverage Zone File** drop-down list, choose a Coverage Zone file.

- Step 3** In the **DNS TTL** field, configure the time period (in seconds) for caching DNS replies. Enter a number from 0 to 60. The default is 60 seconds.
- Step 4** Click **Submit** to save settings.

**Tip**

To apply a Coverage Zone file to an individual SR for local coverage zone configuration, see the [“Configuring Service Router Settings” section on page 5-109](#).

## Where to Go Next

See the following support documentation:

- For information about system output logs, see the [“System Audit Logs” section on page 10-6](#).
- For information on upgrading the ECDS software, see the [“Upgrading Software” section on page 11-1](#).
- For information on the ports used by the ECDS, see the [“System Port Numbers” section on page 10-7](#).

**Tip**

For the most current information, refer to the Cisco ECDS 2.5 Software Administration Configuration Guide on Cisco.com.



# CHAPTER 10

## Monitoring the Enterprise CDS

---

The following sections describe how to use CDSM tools for system monitoring and system diagnostics:

- [System Monitoring, page 10-1](#)
- [Device Monitoring, page 10-9](#)
- [Viewing Reports, page 10-22](#)
- [Delivery Service Monitoring, page 10-27](#)
- [Viewing Statistics, page 10-37](#)
- [Managing Transaction Logs, page 10-41](#)
- [Where to Go Next, page 10-64](#)

### System Monitoring

System monitoring consists of the following:

- [System Status, page 10-1](#)
- [System Home Page, page 10-4](#)
- [System Audit Logs, page 10-6](#)
- [System Port Numbers, page 10-7](#)

### System Status

The CDSM displays the system status in the System Status bar that is located above the navigation tabs in every window. The System Status bar presents the overall device, content health of the system, and license alerts and helps you immediately identify any problems on the network. Use this feature to monitor devices, content replication, and license alerts in your ECDS network.

The system status reporting mechanism uses four alarm lights to identify problems that need to be resolved. Each light represents a different alarm level, as follows:

- Green—No alarms (the system is in excellent health)
- Yellow—Minor alarms
- Orange—Major alarms
- Red—Critical alarms

When you roll your mouse over an alarm light in the System Status bar, a pop-up message provides further details about the device, delivery service, or license status. See [Figure 10-1](#).

Figure 10-1 System Status Bar



When you click the alarm light, a new window opens (Troubleshooting Devices or Troubleshooting Service Alerts), listing the individual devices, delivery services, or licenses that need attention.

When you roll your mouse over an item under the Alarm Information column in the Troubleshooting Devices or Troubleshooting Services window, the Troubleshooting Tools menu is displayed. The Troubleshooting Tools menu provides links to all the diagnostic tools, troubleshooting tools, and monitoring applications for troubleshooting and resolving the problem. [Figure 10-2](#) shows the Troubleshooting Tools menu for device alarms.

Figure 10-2 Troubleshooting Tools Menu

| Troubleshooting Devices |            |        |          |                                                                                              | Alarms: 5 Minor, 5 Major, 0 Critical |  | Rows: 10 |
|-------------------------|------------|--------|----------|----------------------------------------------------------------------------------------------|--------------------------------------|--|----------|
| Device Name             | IP Address | Status | Severity | Alarm Information                                                                            | Time                                 |  |          |
| DD4-CDE220-2            | 8.1.0.3    | Online | Major    | SE U1-2S3-1 keepalive timed-out                                                              | Sat May 15 00:35:16 GMT 2010         |  |          |
| DD4-FIBER-1             | 8.1.0.8    | Online | Major    | SE DD4-FIBER-1 keep                                                                          | Sat May 15 00:35:16 GMT 2010         |  |          |
| U1-2S3-1                | 7.5.1.13   | Online | Major    | Device clock is not syn                                                                      | Sat May 15 00:35:40 GMT 2010         |  |          |
| DD4-FIBER-1             | 8.1.0.8    | Online | Major    | Core file(s) detected                                                                        | Fri May 07 19:51:10 GMT 2010         |  |          |
| DD4-FIBER-1             | 8.1.0.8    | Online | Major    | Interface GigabitEthernet 5/0 is down.                                                       | Wed May 12 00:21:33 GMT 2010         |  |          |
| DD4-CDE220-2            | 8.1.0.3    | Online | Minor    | A power supply power cable is unplugged or the psu failed.                                   | Sat May 15 00:32:59 GMT 2010         |  |          |
| DD4-CDE220-2            | 8.1.0.3    | Online | Minor    | "Device: /dev/sdd, 1 Currently unreadable (pending) sectors"                                 | Sat May 15 00:34:49 GMT 2010         |  |          |
| U1-2S3-1                | 7.5.1.13   | Online | Minor    | A power supply power cable is unplugged or the psu failed.                                   | Tue Mar 16 21:03:40 GMT 2010         |  |          |
| DD4-CDE205-1            | 8.1.0.5    | Online | Minor    | Some content or crawl jobs of delivery service:HTTP are failed to be acquired or replicated. | Thu May 13 19:13:55 GMT 2010         |  |          |
| DD4-FIBER-1             | 8.1.0.8    | Online | Minor    | A power supply power cable is unplugged or the psu failed.                                   | Fri May 07 00:59:16 GMT 2010         |  |          |

<< Page 1 >> Showing 1-10 of 10 Rows, 4 of 4 Devices with Alarms

207304

## Device Alarms

Device alarms are associated with applications and services running on SEs, SRs, and CDSMs. Device alarms are defined by the reporting application or service. For example, the SR raises an alarm for an SE (the keep-alive timed out alarm) if the SE has a Layer 3 failure. Device alarms can also reflect reporting problems between the device and the CDSM. [Table 10-1](#) describes the alarms.

Alarm thresholds are configured for each device. For more information, see the “[Setting Service Monitor Thresholds](#)” section on [page 5-97](#).



**Table 10-1**      **Device Alarms for Reporting Problems**

| Alarm              | Alarm Severity | Device Status | Description                                                    |
|--------------------|----------------|---------------|----------------------------------------------------------------|
| Device is offline  | Critical       | Offline       | The device has failed to communicate with the CDSM.            |
| Device is pending  | Major          | Pending       | The device status cannot be determined.                        |
| Device is inactive | Minor          | Inactive      | The device has not yet been activated or accepted by the CDSM. |

To troubleshoot a device from the System Status bar:

- 
- Step 1** Click the **Devices** alarm light or click the **Device** link. The Troubleshooting Devices window is displayed.
- Step 2** In the Alarm Information column, hold your mouse over the alarm message until the Troubleshooting Tools menu is displayed. See [Figure 10-2](#).
- Step 3** Click the troubleshooting tool you want to use. The link takes you to the corresponding page in the CDSM. [Table 10-2](#) describes the tools available for all device alarms.

**Table 10-2**      **Troubleshooting Tools for Device Alarms**

| Item                | Navigation                                                                        | Description                                            |
|---------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------|
| Edit/Monitor Device | Devices home page                                                                 | Displays Devices home page                             |
| Telnet to Device    | Opens a Telnet window                                                             | Initiates a Telnet session using the device IP address |
| Run Show Commands   | <b>Devices &gt; Device Monitoring &gt; Show/Clear Commands &gt; Show Commands</b> | Displays device <b>show</b> command tool               |

## Service Alarms

Service alarms for content replication problems and are associated with delivery services. Service alarms are raised by the CDSM based on replication status reports, or by the SE health manager based on acquisition and distribution errors.

If the same fault is reported by the replication status and by the SE health manager, the CDSM reports both; one appears as the true alarm and the other as an error. The CDSM does not correlate nor attempt to consolidate the errors generated by the replication status and by the SE health manager.

To troubleshoot service replication issues from the System Status bar:

- 
- Step 1** Click the **Services** alarm light or click the **Service** link. The Troubleshooting Services window is displayed. [Table 10-3](#) lists the service alarms.

**Table 10-3**      *Service Alarms for Delivery Service Replication Status*

| Alarm                                           | Severity | Description                                                                                                  |
|-------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------|
| Replication Status is Failed                    | Critical | The number of SEs in the delivery service that failed to replicate the content is greater than zero.         |
| Replication Status is Pending                   | Minor    | The number of SEs in the delivery service with content replication status unknown is greater than zero.      |
| Single content item failed or crawl job failed. | Minor    | A single content failed to be acquired or replicated, or a crawl job failed to acquire or replicate content. |

- Step 2** In the Alarm Information column, hold your mouse over the alarm message until the Troubleshooting Tools menu is displayed.
- Step 3** Click the troubleshooting tool that you want to use. The link takes you to the corresponding page in the CDSM. [Table 10-4](#) describes the tools available for all service alarms.

**Table 10-4**      *Troubleshooting Tools for Content Alarms*

| Item                    | Navigation                                                     | Description                                                     |
|-------------------------|----------------------------------------------------------------|-----------------------------------------------------------------|
| View Replication Status | <b>Services &gt; Delivery Services &gt; Replication Status</b> | Displays second-level replication status for a delivery service |
| Edit Delivery Service   | <b>Services &gt; Delivery Services &gt; Definition</b>         | Opens the Delivery Service Definition page                      |

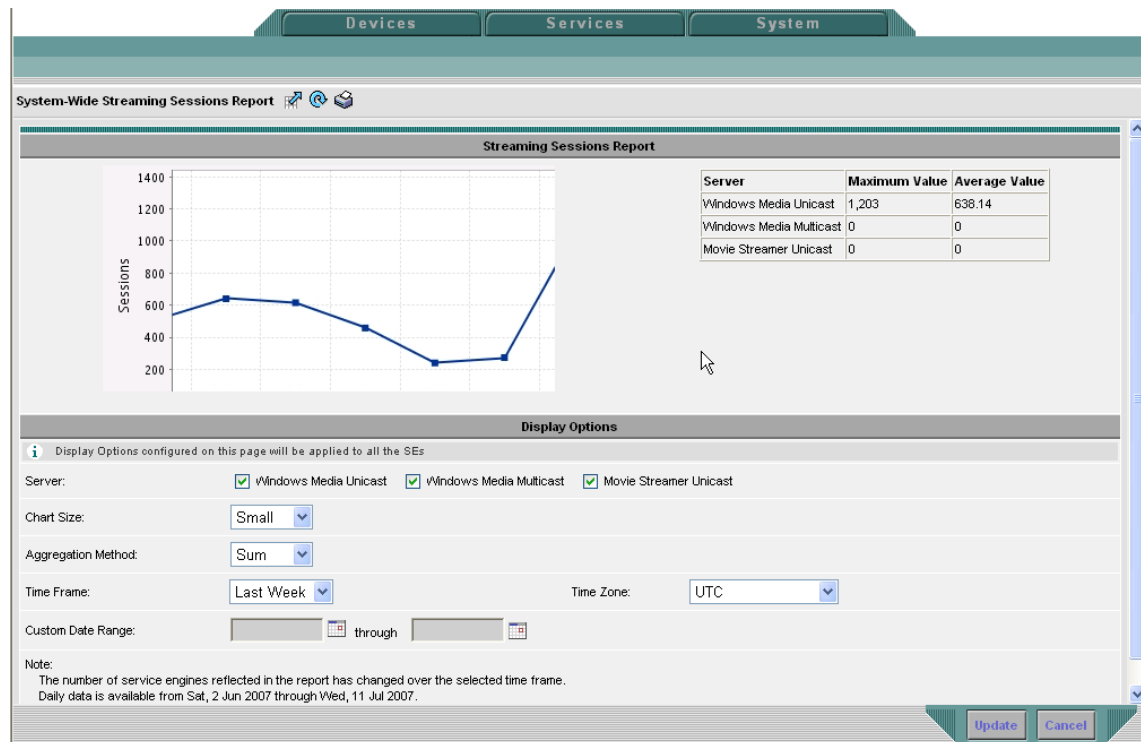
## System Home Page

The System Home page ([Figure 10-3](#)) provides overall system performance graphs, and overall system information on configuration and software versions running on the ECDS devices. Clicking the links for devices, delivery services, and programs take you to the corresponding table pages.

**Figure 10-3**      **System Home Page**

The information displayed in the graphs is based on a snapshot of your ECDS network and represents the state of your SEs at the end of every two polling periods. The following are tips to help you manage the System Home page:

- To refresh the graphs, click the **Refresh** icon next to “System Home.”
- Change the interval between polls by changing the `System.datafeed.pollRate` field in **System > Configuration > System Properties**. The default polling rate is 300 seconds (5 minutes).
- Change the report settings for the System-Wide Bandwidth Served or System-Wide Bandwidth Efficiency Gain graphs by clicking **View Detailed Report**.
- Clicking the **Streaming Sessions** link at the bottom of the home page opens the System-Wide Streaming Sessions Report page, as shown in Figure 10-4. For more information about these reports, see the “Viewing Reports” section on page 10-22.

**Figure 10-4** System-Wide Streaming Sessions Report Page

## System Audit Logs

The CDSM logs user activity in the system. The only activities that are logged are those that change the ECDS network. This feature provides accountability for users actions (who did what and when). Logged activities include the following:

- Creation of ECDS network entities
- Modification and deletion of ECDS network entities
- System configurations

To view audit trail logs:

- 
- Step 1** Choose **System > Logs > Audit Trail Logs**. The Audit Log page is displayed. All logged transactions in the CDSM are listed by date and time, user, actual transaction that was logged, and the IP address of the machine that was used.
- Step 2** To determine the number of rows that you want to display, choose a number from the Rows drop-down list.
-

## System Port Numbers

Information on all the protocols and ports used by the ECDS can be viewed on the CDS-IS Well Known Ports page.

To view ports used by the ECDS, choose **System > CDS-IS Well Known Ports**. The CDS-IS Well Known Ports page is displayed. [Table 10-5](#) lists all ports listed on the CDS-IS Well Known Ports page.

To view all ports on one page, from the **Rows** drop-down list, choose **All**.

**Table 10-5** Enterprise CDS—Well Known Ports

| Source Group       | Destination Group | Protocol | Source Port | Destination Port | Purpose                                                                                                            |
|--------------------|-------------------|----------|-------------|------------------|--------------------------------------------------------------------------------------------------------------------|
| CDSM               | SE                | TCP      | ANY         | 443              | ECDS management (notifications, updates, queries)                                                                  |
| SE                 | CDSM              | TCP      | ANY         | 443              | ECDS management (notifications, updates, queries)                                                                  |
| CDSM               | SR                | TCP      | ANY         | 443              | ECDS management (notifications, updates, queries)                                                                  |
| SR                 | CDSM              | TCP      | ANY         | 443              | ECDS management (notifications, updates, queries)                                                                  |
| CDSM               | CDSM              | TCP      | ANY         | 443              | ECDS management (notifications, updates, queries)                                                                  |
| SE                 | SR                | UDP      | ANY         | 2323             | Service Engine to Service Router keepalives                                                                        |
| SE                 | CDSM              | UDP      | ANY         | 2000             | Service Engine to CDSM keepalives                                                                                  |
| SR                 | CDSM              | UDP      | ANY         | 2000             | Service Router to CDSM keepalives                                                                                  |
| SE                 | SE                | TCP      | ANY         | 554              | RTSP requests between Service Engines                                                                              |
| SE                 | SE                | TCP      | ANY         | 80               | HTTP request between Service Engines                                                                               |
| SE                 | SE                | TCP      | ANY         | 5262             | Metadata receiver in Service Engine                                                                                |
| SE                 | SE                | TCP      | ANY         | 5263             | Metadata sender in Service Engine                                                                                  |
| SE                 | SE                | TCP      | ANY         | 5264             | Unicast receiver in Service Engine                                                                                 |
| SE                 | SE                | TCP      | ANY         | 5271             | Metadata receiver in Service Engine                                                                                |
| SE                 | SE                | TCP      | ANY         | 1935             | Flash Media Streaming live and interactive applications                                                            |
| SE                 | SE                | TCP      | ANY         | 80               | Flash Media Streaming VOD file requests by way of HTTP                                                             |
| CDSM               | SE                | TCP      | ANY         | 10999            | For Remote Method Invocation (RMI) over Secure Socket Layer (SSL).Used by the Resources, Events, and Agents (REA). |
| Administrator (PC) | CDSM              | TCP      | ANY         | 8443             | Access to CDSM GUI from administrator PC                                                                           |

**Table 10-5** Enterprise CDS—Well Known Ports (continued)

| Source Group       | Destination Group | Protocol | Source Port | Destination Port | Purpose                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|-------------------|----------|-------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrator (PC) | SE                | TCP      | Any         | 1111             | Flash Media Streaming fmsadmin process listens on port 1111 for administrator APIs that are used to access the Flash Media Server that is part of the Flash Media Streaming protocol engine. Port 1111 is only open to the FMS admin hosts that are configured in the FMS Admin Allow Hosts page. See the <a href="#">“Configuring the FMS Administrator” section on page 5-38</a> . |
| Subscriber (PC)    | DNS Server/Proxy  | UDP      | ANY         | 53               | DNS query for Service Router Fully-Qualified Domain Name (SRFQDN) from subscriber (PC)                                                                                                                                                                                                                                                                                               |
| Subscriber (PC)    | SR                | TCP      | ANY         | 80               | HTTP request to Service Router from subscriber (PC)                                                                                                                                                                                                                                                                                                                                  |
| Subscriber (PC)    | SR                | TCP      | ANY         | 554              | RTSP request to Service Router from subscriber (PC)                                                                                                                                                                                                                                                                                                                                  |
| Subscriber (PC)    | SR                | TCP      | ANY         | 1935             | RTMP (Flash Media Streaming) request to Service Router from subscriber (PC)                                                                                                                                                                                                                                                                                                          |
| Subscriber (PC)    | SE                | TCP      | ANY         | 80               | HTTP request to Service Engine from subscriber (PC)                                                                                                                                                                                                                                                                                                                                  |
| Subscriber (PC)    | SE                | TCP      | ANY         | 554              | RTSP request to Service Engine from subscriber (PC)                                                                                                                                                                                                                                                                                                                                  |
| Subscriber (PC)    | SE                | TCP      | ANY         | 1935             | RTMP (Flash Media Streaming) request to Service Engine from subscriber (PC)                                                                                                                                                                                                                                                                                                          |
| Subscriber (PC)    | SE                | TCP      | ANY         | 1755             | MMS request to Service Engine from subscriber (PC)                                                                                                                                                                                                                                                                                                                                   |
| All Devices        | NTP Servers       | UDP      | ANY         | 123              | Query time servers                                                                                                                                                                                                                                                                                                                                                                   |
| All Devices        | NMS Servers       | TCP      | ANY         | 161              | SNMP query or polling                                                                                                                                                                                                                                                                                                                                                                |
| All Devices        | NMS Servers       | UDP      | ANY         | 162              | SNMP trap                                                                                                                                                                                                                                                                                                                                                                            |
| All Device         | Syslog Server     | UDP      | ANY         | 514              | Syslog                                                                                                                                                                                                                                                                                                                                                                               |
| SE                 | Origin Servers    | TCP      | ANY         | 80               | Acquire content from Origin Servers using HTTP                                                                                                                                                                                                                                                                                                                                       |
| SE                 | Origin Servers    | TCP      | ANY         | 443              | Acquire content from Origin Servers using HTTPS                                                                                                                                                                                                                                                                                                                                      |
| SE                 | Origin Servers    | TCP      | ANY         | 21               | Acquire content from Origin Servers using FTP                                                                                                                                                                                                                                                                                                                                        |
| SE                 | Origin Servers    | TCP      | ANY         | 139              | Acquire content from Origin Servers using SMB                                                                                                                                                                                                                                                                                                                                        |
| SE                 | Origin Servers    | TCP      | ANY         | 80               | Get Flash Media Streaming VOD content from Origin server by using HTTP                                                                                                                                                                                                                                                                                                               |
| SE                 | Origin Servers    | TCP      | ANY         | 1935             | Get Flash Media Streaming live stream from active Content Acquirer or proxy interactive application data from edge SE to Origin Server using RTMP                                                                                                                                                                                                                                    |

# Device Monitoring

This section describes the following topics:

- [Devices Table, page 10-9](#)
- [Devices Home Page, page 10-11](#)
- [Using the CDSM Show/Clear Commands Tool, page 10-12](#)
- [CPU Utilization, page 10-22](#)

For more detailed statistics on HTTP, Web Media, Movie Streamer, and Flash Media Streaming traffic, see the [“Viewing Statistics” section on page 10-37](#).

## Devices Table

The Devices Table page displays all devices registered in the ECDS network ([Figure 10-5](#)).

**Figure 10-5**      **Devices Table Page**

| Device Name  | Type                                      | IP Address | Status  | Location             | Software Version |
|--------------|-------------------------------------------|------------|---------|----------------------|------------------|
| NE-612-12    | Service Engine                            | 3.1.4.31   | Online  | NE-612-12-location   | 2.0.0.b.410      |
| NE-612-5     | Service Engine                            | 3.1.4.14   | Online  | tier-1               | 2.0.0.b.400      |
| NE-612-6     | Service Engine                            | 3.1.4.15   | Online  | tier-2               | 2.0.0.b.430      |
| NE-612-7     | Service Engine                            | 3.1.4.16   | Online  | tier-1               | 2.0.0.b.430      |
| NE-7326-2    | Service Engine                            | 3.1.4.21   | Online  | tier-3               | 2.0.0.b.430      |
| NE-CDM-612-9 | Content Delivery System Manager (Primary) | 3.1.4.18   | Online  |                      | 2.0.0.b.430      |
| NE-CR-612-4  | Service Router                            | 3.1.4.13   | Online  | tier-1               | 2.0.0.b.430      |
| Q5-CDE200-1  | Service Engine                            | 2.225.2.11 | Offline | tier-1               | 2.0.0.b.410      |
| Q5-CDE200-2  | Service Engine                            | 2.225.2.56 | Online  | Q5-CDE200-2-location | 2.0.0.b.420      |
| Q6-CDE200-1  | Service Engine                            | 2.225.2.15 | Offline | Q6-CDE200-1-location | 2.0.0.b.420      |

[Table 10-6](#) describes the Device Table columns. You can sort the information in the table by clicking on any column title. The table can be sorted in ascending or descending order for each column.

The table defaults to listing ten rows. You can change the number of rows by clicking the Rows drop-down list. The bottom of the table lists the page number and the total number of pages, as well as how many items are showing out of the total number of items.

**Table 10-6**      **Device Table Columns**

| Column Heading | Description                                            |
|----------------|--------------------------------------------------------|
| Device Name    | Host name of the device.                               |
| Type           | Device type: SE, SR, CDSM (Primary), CDSM (Secondary). |
| IP Address     | Primary IP address of the device.                      |

**Table 10-6**      **Device Table Columns (continued)**

| Column Heading   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status           | <p>Status is one of the following:</p> <ul style="list-style-type: none"> <li>• Online—Device has been activated through the CDSM and is able to send and receive data and control traffic.</li> <li>• Offline—Device has failed to communicate with the CDSM.</li> <li>• Pending—Device status cannot be determined. The device could be in the process of being activated by the CDSM</li> <li>• Offloading—Device is in the Server Offload state. To monitor the current streams on an SE during the Server Offload state, view the statistics for each protocol engine (for example, Movie Streamer), specifically the fields noted in <a href="#">Table 10-26 on page 10-38</a>. Once all protocol engines have finished streaming, you can perform maintenance or upgrade the software on the device. For information about upgrading the software, see the <a href="#">“Upgrading Software” section on page 11-1</a>.</li> </ul> |
| Location         | Location the device is assigned to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Software Version | Device software version.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

[Table 10-7](#) describes the icons for the device table. To view or modify the configuration of a device, click the **Edit** icon next to the device name.

**Table 10-7**      **Device Table Icons**

| Icon                                                                                | Function                                                                                        |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
|  | Activate all inactive Service Engines.                                                          |
|  | Edit the device.                                                                                |
|  | Export a table to a comma-separated value (CSV) file.                                           |
|  | Create a filtered table. Filter the devices by the device name, device type, and device status. |
|  | View all devices. Click this icon to view all devices after you have created a filtered table.  |
|  | Refresh the table                                                                               |
|  | Print the current window.                                                                       |

For more information, see the [“Devices, Services, and Other Tables” section on page 3-7](#) of [Chapter 3, “Getting Started.”](#)



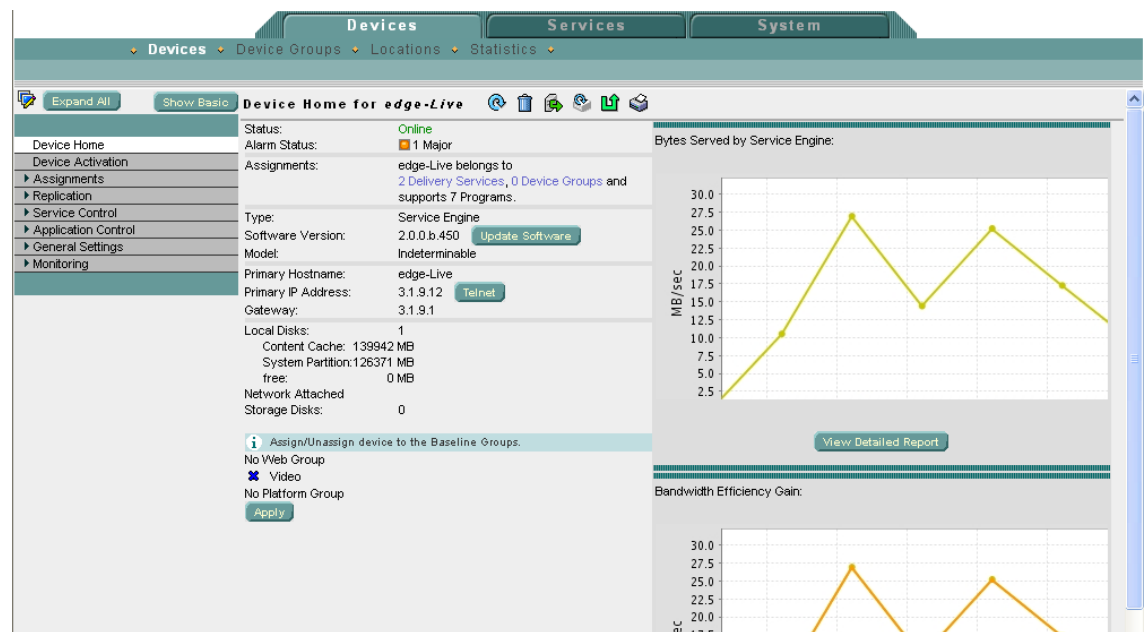
## Devices Home Page

The Devices home page (Figure 10-6) provides alarm status and information on the device. Only basic information is displayed for the SR and CDSM.

By clicking the **Delivery Services** and **Device Groups** links in the Assignments area on the home page for an SE a table is displayed listing all the delivery services or device groups in the ECDS, and which ones the SE is assigned to. Through this page, you can assign the device to additional delivery services or device groups by clicking the icon next to the applicable delivery services or device groups and submitting your selection.

You can update the device software, access the device management interface, and telnet to the device from the Devices home page. For more information about updating the software, see the “[Upgrading Software](#)” section on page 11-1 of Chapter 11, “[Maintaining the Enterprise CDS](#).”

**Figure 10-6 SE Devices Home Page**



The Bandwidth Served by Service Engine and the Bandwidth Efficiency Gain graphs are also displayed. For more information, see the “[Viewing Reports](#)” section on page 10-22.

The Devices home page for an SE or an SR provides several icons. Table 10-8 describes these icons. The CDSM home page has a subset of the icons.

**Table 10-8** *SE Devices Home Page Icons*

| Icon                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Displays all devices. Clicking this icon displays a list of the Service Engines. To view or configure another Service Engine, click the Service Engine name. The configuration page for that device is displayed and the left-panel menu displays. This feature allows you to compare the configuration on different Service Engines. To return to the left-panel menu, click the <b>Display Menu</b> icon.                                                                          |
|    | Displays the left-panel menu for the device.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|    | Refreshes the page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|    | Deletes the device. See the “ <a href="#">Deleting a Device</a> ” section on page 11-10 of <a href="#">Chapter 11</a> , “ <a href="#">Maintaining the Enterprise CDS</a> .”                                                                                                                                                                                                                                                                                                          |
|    | Updates application statistics. The device statistics are updated at a configurable time interval, which is set in the System Configuration page (System.monitoring.collectRate). To see the latest statistics immediately, without waiting for the time interval to elapse, click this icon. To configure the time interval, see the “ <a href="#">Configuring System Settings</a> ” section on page 9-7 of <a href="#">Chapter 9</a> , “ <a href="#">Configuring the System</a> .” |
|   | Forces a full database update from the CDSM to the SE. If the CDSM and SE databases are not synchronized because of network errors or other errors, you can synchronize them by clicking this icon.                                                                                                                                                                                                                                                                                  |
|  | Reboots the device. See the “ <a href="#">Rebooting Devices</a> ” section on page 11-9.                                                                                                                                                                                                                                                                                                                                                                                              |
|  | Prints the home page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

For more information about the Devices home page, see the “[Devices Home Page](#)” section on page 3-8 of [Chapter 3](#), “[Getting Started](#).”

## Using the CDSM Show/Clear Commands Tool

The **show** and **clear** commands provide detailed device monitoring. See the **show** commands in [Table 10-9](#) and the **clear** commands in [Table 10-10](#). A full list of **show** and **clear** commands is available from the drop-down list on the respective command page.

To use the CDSM **show** or **clear** command tool:

- 
- Step 1** Choose **Devices > Devices > Monitoring > Show/Clear Commands** and then click either **Show Commands** or **Clear Commands**:
- [Show Commands](#)
  - [Clear Commands](#)
- Step 2** From the drop-down list, choose a command.

- Step 3** Enter arguments for the command, if any.
- Step 4** Click **Submit** to display the command output. The results of the command are displayed in a new window.

## Show Commands

Table 10-9 lists available **show** commands. See the “[show Command Examples](#)” section on page 10-20.

**Table 10-9** *show Command Arguments*

| show Command   | Arguments                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Device       | Description                                                              |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|--------------------------------------------------------------------------|
| access-list    | { 300 }                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | SE           | Access control list (ACL) configuration                                  |
| acquirer       | [ <b>delivery-service</b> [ <b>delivery-service-id</b> <i>delivery-service-num</i>   <b>delivery-service-name</b> <i>delivery-service-name</i> ]   <b>progress</b> [ <b>delivery-service-id</b> <i>delivery-service-num</i>   <b>delivery-service-name</b> <i>delivery-service-name</i> ]   <b>proxy authentication</b> ]                                                                                                                                                         | SE           | Acquirer information and progress for a specified channel number or name |
| alarms         | [ <b>critical</b>   <b>detail</b>   <b>history</b>   <b>major</b>   <b>minor</b>   <b>status</b> ]                                                                                                                                                                                                                                                                                                                                                                                | SE, SR, CDSM | Alarm status and history                                                 |
| arp            | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |              | Address Resolution Protocol (ARP) table                                  |
| authentication | { <b>user</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | SE, SR, CDSM | Authentication configuration                                             |
| authsvr        | [ <b>location-server</b>   <b>unknown-server</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                |              | Authorization server status                                              |
| bandwidth      | [ <b>flash-media-streaming</b>   <b>movie-streamer</b>   <b>wmt</b> ]                                                                                                                                                                                                                                                                                                                                                                                                             | SE           | Bandwidth allocated to a particular device                               |
| banner         | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |              | Banner information                                                       |
| bitrate        | [ <b>wmt</b>   <b>movie-streamer</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                            | SE           | Bit rate allocated to a particular device                                |
| cache          | [ <b>content</b> <i>1-1000</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                  | SE           | Cache content list                                                       |
| capability     | { <b>profile</b> <i>1-65535</i> }                                                                                                                                                                                                                                                                                                                                                                                                                                                 | SE           | Cap-X profile ID                                                         |
| cdn-select     | Not supported                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | SR           | —                                                                        |
| cdn-statistics | { <b>flash-media-streaming</b> { <b>device-group-name</b> <i>device-group-name</i>   <b>device-groups</b>   <b>service-engines</b> } <b>movie-streamer</b> { <b>service-engines</b>   <b>device-group-name</b> <i>groupname</i>   <b>device-groups</b> }   <b>http</b> { <b>service-engines</b>   <b>device-group-name</b> <i>groupname</i>   <b>device-groups</b> }   <b>wmt</b> { <b>service-engines</b>   <b>device-group-name</b> <i>groupname</i>   <b>device-groups</b> } } | CDSM         | —                                                                        |

Table 10-9 show Command Arguments (continued)

| show Command          | Arguments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Device       | Description                                                                                                                      |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------|
| cdnfs                 | { <b>usage</b>   <b>volumes</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | SE           | CDS network file system (cdnfs) information                                                                                      |
| clock                 | [ <b>detail</b>   <b>standard-timezones</b> { <b>all</b>   <b>details</b> <i>timezone</i>   <b>regions</b>   <b>zones</b> <i>region-name</i> } ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | SE, SR, CDSM | Controls the system clock                                                                                                        |
| cms                   | { <b>database</b> { <b>content</b> { <b>dump</b> <i>filename</i>   <b>text</b>   <b>xml</b> }   <b>maintenance</b> [ <b>detail</b> ] }   <b>info</b>   <b>processes</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | SE, SR, CDSM | Centralized Management System (CMS) embedded database content and maintenance status                                             |
| content               | { <b>all</b>   <b>url</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | SE           | All content entries in the CDS                                                                                                   |
| device-mode           | { <b>configured</b>   <b>current</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | SE, SR, CDSM | Configured or current mode of a device                                                                                           |
| direct-server-return  | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | —            | Direct Server return information                                                                                                 |
| disks                 | [ <b>current</b>   <b>details</b>   <b>failed-sectors</b> [ <i>disk_name</i> ]   <b>raid-state</b>   <b>SMART-info</b> [ <b>details</b> ] ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | SE, SR, CDSM | Disk information                                                                                                                 |
| distribution          | [ <b>delivery-services</b> [ <b>delivery-service-id</b> <i>delivery-service-num</i>   <b>delivery-service-name</b> <i>delivery-service-name</i> ] ]<br><br>[ <b>forwarder-list</b> [ <b>delivery-service-id</b> <i>delivery-service-num</i> [ <b>detail</b> ]   <b>delivery-service-name</b> <i>delivery-service-name</i> [ <b>detail</b> ]   <b>detail</b> ] ]<br><br>[ <b>location</b> { <b>forwarder-load-weight</b>   <b>live-load-weight</b>   <b>location-leader-preference</b> } [ <b>delivery-service-id</b> <i>delivery-service-num</i>   <b>delivery-service-name</b> <i>delivery-service-name</i> ] ]<br><br>[ <b>object-status</b> <i>object-url</i> ]<br><br>[ <b>processes</b>   <b>remote</b> ]<br><br>[ <b>remote</b> <i>ip-address</i> { <b>metadata-sender</b> <b>delivery-service-id</b> <i>delivery-service-num</i> [ <b>start-generation-id</b> <i>gen-id</i>   <b>end-generation-id</b> <i>gen-id</i> ]   <b>unicast-sender</b> <b>delivery-service-id</b> <i>delivery-service-num</i> { <b>cdn-url</b> <i>cdn_url</i>   <b>probe</b>   <b>relative-cdn-url</b> <i>cdn_url</i> } } ]<br><br>[ <b>remote traceroute</b> { <b>forwarder-next-hop</b> <b>delivery-service-id</b> <i>delivery-service-num</i> { <b>max-hop</b> <i>maxhop_num</i>   <b>trace-till-good</b>   <b>trace-till-root</b> }   <b>unicast-sender</b> <b>delivery-service-id</b> <i>delivery-service-num</i> { <b>cdn-url</b> <i>cdn_url</i>   <b>probe</b>   <b>relative-cdn-url</b> <i>cdn_url</i> } { <b>max-hop</b> <i>maxhop_num</i>   <b>trace-till-good</b>   <b>trace-till-root</b> } } ] | SE, SR       | Distribution information for a specified delivery service, probe a remote SE for the liveness of its associated delivery service |
| flash                 | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | —            | Flash memory version and usage information                                                                                       |
| flash-media-streaming | [ <b>license</b> [ <b>logging</b> <i>filename</i>   <b>mtrack</b> ]   <b>stream-status</b> <b>live</b> [ <b>all</b> <i>filename</i> ] ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | SE, SR       | Flash Media Streaming information                                                                                                |

Table 10-9 show Command Arguments (continued)

| show Command       | Arguments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Device       | Description                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|---------------------------------------------------------------|
| ftp                | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | —            | File Transfer Protocol (FTP) caching configuration            |
| hardware           | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | —            | System hardware status                                        |
| hosts              | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | —            | View the hosts on your SE                                     |
| http               | { <b>age-mult</b>   <b>all</b>   <b>cache-cookie</b>   <b>cache-on-abort</b>   <b>object</b>   <b>proxy</b>   <b>reval-each-request</b>   <b>ttl</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | SE           | HTTP caching parameters                                       |
| interface          | { <b>GigabitEthernet</b> <i>slot/port</i>   <b>ide</b> <i>control_num</i>   <b>PortChannel</b> <i>port-num</i>   <b>scsi</b> <i>device_num</i>   <b>Standby</b> <i>group_num</i>   <b>usb</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | SE, SR, CDSM | Hardware interface information                                |
| inventory          | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | —            | System inventory information                                  |
| ip                 | On SE or CDSM: { <b>access-list</b> [ <i>acl-name</i>   <i>acl-num</i> ]   <b>routes</b> }<br>On SR: { <b>access-list</b> [ <i>acl-name</i>   <i>acl-num</i> ]   <b>bgp</b> { <i>ip-prefix</i>   <i>network-ip-address</i>   <b>all</b>   <b>community</b> [ <i>location-community</i> ]   <b>ipv4</b> <b>unicast</b>   <b>memory</b>   <b>neighbors</b> [ <i>neighbor-ip-address</i> ]   <b>nexthop-database</b>   <b>summary</b> }   <b>interface</b> <b>brief</b>   <b>ospf</b> [ <b>border-routers</b>   <b>database</b> [ <b>adv-router</b> <i>ip-address-advertising-router</i>   <b>asbr-summary</b> [ <i>ip-address-link-state-id</i>   <b>detail</b> ]   <b>database-summary</b>   <b>detail</b>   <b>external</b> [ <i>ip-address-link-state-id</i>   <b>detail</b> ]   <b>network</b> [ <i>ip-address-link-state-id</i>   <b>detail</b> ]   <b>nssa-external</b> [ <i>ip-address-link-state-id</i>   <b>detail</b> ]   <b>router</b> [ <i>ip-address-link-state-id</i>   <b>detail</b> ]   <b>self-originated</b> [ <b>detail</b> ]   <b>summary</b> [ <i>ip-address-link-state-id</i>   <b>detail</b> ]   <b>interface</b>   <b>memory</b>   <b>neighbor</b> [ <i>ip-address-neighbor</i> [ <b>detail</b> ]   <b>detail</b>   <b>summary</b> ]   <b>request-list</b> <i>ip-address-neighbor-router</i> { <b>GigabitEthernet</b> <i>slot/port</i>   <b>PortChannel</b> <i>channel-number</i> }   <b>retransmission-list</b> { <b>GigabitEthernet</b> <i>slot/port</i>   <b>PortChannel</b> <i>channel-number</i> }   <b>route</b> [ <i>single-ip-route</i> ]   <b>rsfpf</b> <b>route</b> [ <i>ip-address-advertising-router</i> ]   <b>traffic</b> ]   <b>proximity</b> { <b>algorithm</b>   <b>server</b> }   <b>rib</b> { <b>clients</b> [ <i>single-client</i> ]   <b>memory</b>   <b>recursive-next-hop</b> [ <i>ip-address-next-virtual-hop</i> ]   <b>route</b> [ <i>ip-address-single-route</i>   <b>bgp</b>   <b>direct</b>   <b>isis</b>   <b>ospf</b>   <b>summary</b> ]   <b>unresolved-next-hop</b> [ <i>ip-address-unresolved-next-hop</i> ] }   <b>route</b> } | SE, SR, CDSM | Applied access lists                                          |
| isis               | <b>adjacency</b> { <b>all</b>   <b>GigabitEthernet</b> <i>slot/port</i>   <b>PortChannel</b> <i>channel-number</i> }   <b>ip</b> <b>rsfpf</b> <b>route</b> [ <i>lsp-id</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | SR           | Intermediate System-to-Intermediate System (ISIS) information |
| logging            | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | —            | System message log configuration                              |
| movie-streamer     | [ <b>bandwidth</b>   <b>cache</b>   <b>proxy</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | SE           | Movie Streamer configuration                                  |
| network-filesystem | { <b>client</b> { <b>all</b>   <b>cifs</b>   <b>nfs</b>   <b>samba</b> }   <b>server</b> { <b>nfs</b> } }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | SE           | —                                                             |

Table 10-9 show Command Arguments (continued)

| show Command    | Arguments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Device       | Description                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------------------------------------|
| ntp             | {status}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | SE, SR, CDSM | Network Time Protocol (NTP) parameters                    |
| processes       | [cpu   debug <i>pid</i>   memory   system [delay 1-60   count 1-100]]                                                                                                                                                                                                                                                                                                                                                                                                                                             | SE, SR, CDSM | CPU or memory processes                                   |
| programs        | [movie-streamer [cli   live   rebroadcast]   program-id <i>program-id</i>   program-name <i>program-name</i>   wmt [cli   live   rebroadcast]                                                                                                                                                                                                                                                                                                                                                                     | SE           | List of programs on the SE                                |
| qos             | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | SR           | Quality of Service (QoS) information                      |
| radius server   | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | SE           | RADIUS information                                        |
| rcp             | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |              | Remote file copy information                              |
| rea             | {info}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | SE           | Remote execution agent (REA) information                  |
| rtsp            | {gateway}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | SE           | Real-Time Streaming Protocol (RTSP) configurations        |
| rule            | {action [all [protocol {http   rtmp   rtsp}]   allow [protocol {http   rtmp   rtsp}]   block [protocol {http   rtmp   rtsp}]   generate-url-signature [protocol {http   rtmp   rtsp}]   no-cache [protocol {http   rtmp   rtsp}]   protocol {http   rtmp   rtsp}   redirect [protocol {http   rtmp   rtsp}]   refresh [protocol {http   rtmp   rtsp}]   rewrite [protocol {http   rtmp   rtsp}]   validate-url-signature [protocol {http   rtmp   rtsp}]]   all   pattern-list {1-512 <i>pattern-type</i>   all}} | SE           | Rules configuration information                           |
| running-config  | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |              | Current running configuration information on the terminal |
| service-monitor | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |              | Service monitor configuration                             |
| service-router  | On SE: {keepalive-interval   service-monitor}<br>On SR: {access-policy   content-based-routing   dns-ttl   forwarding [content-origin <i>content-origin</i> ]   lastresort [domain <i>domain-name</i> ]   load {all   sename <i>sename</i> }   proximity-based-routing   redirect-burst-control   redirect-mode   routes [content-origin <i>content-origin</i> ]   service-monitor   services {all   sename <i>sename</i>   summary [content-origin <i>content-origin</i> ]} }<br>On CDSM: {service-monitor}      | SE, SR, CDSM | Service Router configuration                              |
| services        | {ports [port-num]   summary}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | SE, SR, CDSM | Services-related information                              |

Table 10-9 show Command Arguments (continued)

| show Command   | Arguments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Device       | Description                                        |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------------------------------------------------|
| snmp           | { <b>alarm-history</b>   <b>engine ID</b>   <b>group</b>   <b>stats</b>   <b>user</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | SE, SR, CDSM | Simple Network Management Protocol (SNMP) status   |
| srp            | { <b>database</b> { <i>key-hex-string</i>   <b>brief</b>   <b>content</b>   <b>group</b>   <b>maincontent</b> <i>target-string</i>   <b>record</b> <i>key-hex-string</i>   <b>service</b>   <b>size</b> <i>low high</i>   <b>statistics</b>   <b>subid</b> <i>key-hex-string target-string</i>   <b>update</b> <i>start end</i> }   <b>leafset</b>   <b>memory</b>   <b>multicast database</b> [ <b>brief</b>   <b>statistics</b>   <i>group-id</i> [ <i>elements start end</i> ]   <b>message</b> <i>target-string</i>   <b>sender</b> <i>key-hex-string</i> ]   <b>neighbor</b> [ <b>detail</b>   <b>down</b> ]   <b>process</b>   <b>route</b> [ <b>backup</b>   <b>statistics</b> ] <b>subscribers</b> }                                                                                                                                                                                                                                                                                                                                                  |              | Spatial Reuse Protocol (SRP) interface information |
| ssh            | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |              | Secure Shell (SSH) status and configuration        |
| standby        | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |              | Standby interface information                      |
| startup-config |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |              | Startup configuration during initial bootup        |
| statistics     | On all devices: <b>authentication</b>   <b>icmp</b>   <b>ip</b>   <b>netstat</b>   <b>radius</b>   <b>services</b>   <b>snmp</b>   <b>tacacs</b>   <b>tcp</b>   <b>udp</b><br><br>On SR only: { <b>cdn-select summary</b>   <b>ip</b> [ <b>ospf</b>   <b>proximity</b> { <b>rib</b>   <b>server</b> } ]   <b>isis</b> [ <b>GigabitEthernet</b> <i>slot/port</i>   <b>PortChannel</b> <i>channel-number</i> ]   <b>service-registry</b>   <b>service-router</b> { <b>all</b>   <b>content-origin</b> <i>content-origin</i>   <b>dns</b>   <b>history</b>   <b>keepalive</b>   <b>se</b> <i>se-name</i>   <b>summary</b> } <b>srp</b> }<br><br>On CDSM only: <b>content-distribution-network device status</b> <i>device-name or device-group-name or device-ID</i><br><br><b>replication</b> { <b>content-items</b> <i>content-item</i>   <b>delivery-service</b> [ <b>selected-delivery-service</b> <i>content-origin-name</i> ]   <b>item</b> <i>content-item-url</i>   <b>service-engines</b> <b>selected-delivery-service</b> <i>content-origin-name</i> } | SE, SR, CDSM | System statistics                                  |

Table 10-9 *show Command Arguments (continued)*

| show Command | Arguments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Device       | Description                                                                         |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------------------------------------------------------------------------------|
| statistics   | <p>On SE only:</p> <p><b>access-lists</b> 300</p> <p><b>acquirer</b> [contents {<b>delivery-service-id</b> <i>delivery-service-num</i>   <b>delivery-service-name</b> <i>delivery-service-name</i>}   <b>delivery-service-id</b> <i>delivery-service-num</i>   <b>delivery-service-name</b> <i>delivery-service-name</i>   <b>errors</b> {<b>delivery-service-id</b> <i>delivery-service-num</i>   <b>delivery-service-name</b> <i>delivery-service-name</i>}   <b>job-list</b> {<b>delivery-service-id</b> <i>delivery-service-num</i>   <b>delivery-service-name</b> <i>delivery-service-name</i>}]</p> <p><b>authsvr</b>   <b>cdnfs</b></p> <p><b>distribution</b> {<b>all</b>   <b>errors</b> {<b>delivery-service-id</b> <i>delivery-service-num</i>   <b>delivery-service-name</b> <i>name</i>}   <b>metadata-receiver</b>   <b>metadata-sender</b>   <b>unicast-data-receiver</b> [<b>delivery-service-id</b> <i>delivery-service-num</i> [<b>pending-queue</b> <i>num_of_jobs</i>   <b>suspended-queue</b> <i>num_of_jobs</i>   <b>waiting-queue</b> [<b>first</b> [<i>max_jobs</i>]   <b>last</b> [<i>max_jobs</i>]]]   <b>delivery-service-name</b> <i>delivery-service-name</i> [<b>pending-queue</b> <i>num_of_jobs</i>   <b>suspended-queue</b> <i>num_of_jobs</i>   <b>waiting-queue</b> [<b>first</b> [<i>max_jobs</i>]   <b>last</b> [<i>max_jobs</i>]]]   <b>hot-forwarders</b> [<b>forwarder_id</b> <i>forwarder_id</i> {<b>idle-queue</b> [<i>num-of-delivery-services</i>]   <b>priority-queue</b> [<i>num-of-delivery-services</i>]}   <b>forwarder_name</b> <i>forwarder_name</i> {<b>idle-queue</b> [<i>num-of-delivery-services</i>]   <b>priority-queue</b> [<i>num-of-delivery-services</i>]}]}   <b>idle-forwarders</b> [<i>max_idle_forwarders</i>]}   <b>unicast-data-sender</b>}</p> <p><b>flash-media-streaming</b> [<b>connections</b>   <b>dvrcast</b>   <b>errors</b>   <b>livestats</b>   <b>performance</b>   <b>requests</b>]</p> <p><b>http</b> {<b>ims</b>   <b>object</b>   <b>performance</b>   <b>requests</b>   <b>rule</b>}</p> <p><b>movie-streamer</b> {<b>all</b>   <b>bw-usage</b>   <b>errors</b>   <b>performance</b>   <b>requests</b>   <b>rule</b>}   <b>qos policy</b></p> <p><b>replication</b> {<b>content-items</b> <i>content-item</i>   <b>delivery-service</b> [<b>selected-delivery-service</b> <i>content-origin-name</i>]}</p> <p><b>transaction-logs</b>   <b>web-engine</b> [<b>detail</b>]</p> <p><b>wmt</b> {<b>all</b>   <b>bytes</b> {<b>incoming</b>   <b>outgoing</b>}   <b>cache</b>   <b>errors</b>   <b>multicast</b> <i>multicast-station</i>   <b>requests</b>   <b>rule</b>   <b>savings</b>   <b>streamstat</b> [<b>incoming</b>   <b>live</b>   <b>outgoing</b>   <b>stream-id</b> <i>1-999999</i>]   <b>usage</b>}</p> | SE, SR, CDSM |                                                                                     |
| tacacs       | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | —            | TACACS information                                                                  |
| tech-support | [ <b>list-files</b> <i>list-file-directory</i> <b>page</b>   <b>service</b> { <b>acquisition-distribution</b>   <b>authentication</b>   <b>cms</b>   <b>cse</b>   <b>dns</b>   <b>ftp</b>   <b>http</b>   <b>kernel</b>   <b>rules</b>   <b>wmt</b> }]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | SE, SR, CDSM | Information necessary for the Cisco Technical Assistance Center (TAC) to assist you |
| telnet       | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | SE           | Telnet services configuration                                                       |



Table 10-9 show Command Arguments (continued)

| show Command        | Arguments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Device       | Description                                                               |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|---------------------------------------------------------------------------|
| transaction-logging | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |              | Transaction log configuration settings and archived transaction log files |
| url-signature       | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |              | URL signature information                                                 |
| user                | { <b>uid</b> <i>number</i>   <b>username</b> <i>name</i> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | SE, SR, CDSM | User identification number and username information                       |
| users               | { <b>administrative</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | SE, SR, CDSM | Displays users                                                            |
| version             | [ <b>pending</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | SE, SR, CDSM | SE software version information                                           |
| wccp                | <b>show wccp service-engines</b><br><b>show wccp flows</b> { <b>custom-web-cache</b>   <b>dns</b>   <b>ftp-native</b>   <b>https-cache</b>   <b>reverse-proxy</b>   <b>rtsp</b>   <b>service-number</b> <b>service_num</b>   <b>web-cache</b>   <b>wmt</b>   <b>wmt-rtspu</b> } [ <b>summary</b> ]<br><b>show wccp gre</b><br><b>show wccp masks</b> { <b>custom-web-cache</b>   <b>dns</b>   <b>ftp-native</b>   <b>https-cache</b>   <b>reverse-proxy</b>   <b>rtsp</b>   <b>service-number</b> <b>service_num</b>   <b>web-cache</b>   <b>wmt</b>   <b>wmt-rtspu</b> }<br><b>show wccp modules</b><br><b>show wccp port-list</b><br><b>show wccp routers</b><br><b>service-engines</b><br><b>show wccp services</b> [ <b>detail</b> ]<br><b>show wccp slowstart</b> { <b>custom-web-cache</b>   <b>dns</b>   <b>ftp-native</b>   <b>https-cache</b>   <b>reverse-proxy</b>   <b>rtsp</b>   <b>service-number</b> <b>service_num</b>   <b>web-cache</b>   <b>wmt</b>   <b>wmt-rtspu</b> }<br><b>show wccp status</b> |              | WCCP information                                                          |
| web-engine          | <b>all</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | SE           | <b>Note</b> Use the <b>show http</b> command instead                      |
| wmt                 | [ <b>bandwidth</b> [ <b>incoming</b> <b>bypass-list</b> ]   <b>broadcast</b>   <b>detail</b>   <b>diagnostics</b> { <b>header-info</b> { <b>nsc-file</b> <i>nsc-file</i>   <b>stream-file</b> <i>stream-file</i> }   <b>network-trace</b> <i>tcpdump-file</i> }   <b>http</b> <b>allow</b> <b>extension</b>   <b>multicast</b>   <b>proxy</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | SE           | Windows Media Technologies (WMT) bandwidth and proxy mode configuration   |

**Note**

All WMT playable contents can be delivered by either HTTP or RTSP, based on the request. Any content that is cached by the WMT is stored using the RTSP scheme, regardless of whether the content was cached due to an HTTP or RTSP request. Therefore, in the **show** command, the content displays as RTSP.

**show Command Examples****Example 10-1 Monitoring Q-String Caching**

Check for cache-miss and cache hit counters using the **show statistics web-engine** command.

```
U10-2G2-5# sh stat web-engine
HTTP Request Info Statistics

Num Lookups : 2
Preposition Hit : 0
Alien Hit : 0
Cache Hit : 1
Cache Miss : 1
Partial Cache Hit : 0
Cache Bypass : 0
Live Miss : 0
Live Hit : 0
ASX Meta Response : 0
```

## Clear Commands

Table 10-10 lists **clear** command parameters.

**Table 10-10** *clear Command Arguments*

| clear Command | Arguments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Device                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| cache         | { <b>all</b>   <b>content</b> <i>1-1000000</i>   <b>flash-media-streaming</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | SE                               |
| content       | { <b>url</b> <i>url</i> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | SE                               |
| isis          | <b>adjacency</b> { <b>all</b>   <b>GigabitEthernet</b> <i>slot/port</i>   <b>PortChannel</b> <i>channel-number</i> }   <b>ip</b> <b>rsdpf</b> <b>route</b> [ <i>lsp-id</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | SR                               |
| ip            | On all devices: { <b>access-list</b> <b>counters</b> <i>1-99 (standard IP) or 100-199 (extended IP) or access-list-name</i> }<br><br>On SR only: <b>bgp</b> { <i>neighbor-ip-address</i>   <b>all</b> }   <b>ospf</b> { <b>neighbor</b> { <b>all</b>   <b>GigabitEthernet</b> <i>slot/port</i>   <b>PortChannel</b> <i>channel-number</i> }   <b>rsdpf</b> <b>route</b> [ <i>ip-address-advertising-router</i>   <b>traffic</b> ] }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | SE, SR, CDSM                     |
| logging       | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | System message log configuration |
| srp           | <b>database offline</b>   <b>descriptor</b> { <b>all</b>   <i>key-hex-string</i> }   <b>group messages</b>   <b>neighbor</b> { <i>key-hex-string</i>   <i>hostname:port</i> }   <b>resource</b> <i>key-hex-string unicast_resource</i>   <b>route</b> <i>prefix/length</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                  |
| statistics    | On all devices: <b>all</b>   <b>authentication</b>   <b>history</b>   <b>icmp</b>   <b>ip</b>   <b>radius</b>   <b>running</b>   <b>snmp</b>   <b>tacacs</b>   <b>tcp</b>   <b>udp</b><br><br>On CDSM and SE only: <b>distribution</b> { <b>all</b>   <b>metadata-receiver</b>   <b>metadata-sender</b>   <b>unicast-data-receiver</b>   <b>unicast-data-sender</b> }<br><br>On SE and SR only: <b>http</b> { <b>all</b>   <b>ims</b>   <b>object</b>   <b>performance</b>   <b>requests</b>   <b>rule</b> }<br><br>On SR only: <b>ip</b> { <b>ospf</b>   <b>proximity</b> [ <b>rib</b>   <b>server</b> ] }   <b>isis</b>   <b>service-registry</b>   <b>service-router</b>   <b>srp</b> [ <b>replica-set</b> ]<br><br>On SE only: { <b>access-lists</b> <b>300</b>   <b>authsvr</b>   <b>flash-media-streaming</b>   <b>movie-streamer</b>   <b>qos</b> <b>policy-service</b>   <b>rule</b> { <b>action</b> { <b>allow</b>   <b>block</b>   <b>generate-url-signature</b>   <b>no-cache</b>   <b>redirect</b>   <b>refresh</b>   <b>rewrite</b>   <b>validate-url-signature</b> }   <b>all</b>   <b>pattern</b> { <i>1-512</i>   <b>all</b> }   <b>rtsp</b> }   <b>transaction-logs</b>   <b>web-engine</b>   <b>wmt</b> }<br><br><b>Note</b> The <b>clear statistics web-engine</b> and <b>clear statistics all</b> commands only clear normal statistics, not the Web Engine statistics details. To clear all Web Engine statistics, use the <b>clear statistics web-engine force</b> command. | SE, SR, CDSM                     |
| users         | { <b>administrative</b>   <b>request-authenticated</b> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | SE, SR, CDSM                     |
| wmt           | { <b>stream-id</b> <i>1-999999</i> }                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | SE                               |

## CPU Utilization

The CPU Utilization report displays the CPU usage for the SE.

To view the CPU Utilization report for an SE:

- Step 1** Choose **Devices > Devices > Monitoring > Statistics > CPU Utilization**. The CPU Utilization Report page is displayed.
- Step 2** Enter the settings as appropriate. [Table 10-11](#) describes the report settings.

**Table 10-11 CPU Utilization Report Settings**

| Field             | Description                                                                                                                                                                                  |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chart Size        | The chart display size choices are small, medium, or large.                                                                                                                                  |
| Time Frame        | The time frame options are last hour, last day, last week, last month, or custom.                                                                                                            |
| Time Zone         | The time zone choices are SE local time, CDSM local time, or UTC.                                                                                                                            |
| Custom Date Range | The custom date range is used when Time Frame is set to custom. Enter the dates, beginning and end, for the chart in the mm/dd/yyyy format, or choose the dates by using the calendar icons. |

- Step 3** Click **Update** to see the report.

Additional tips:

- To export the report to a CSV (comma-separated value) file, click the **Export** icon in the task bar. A dialog box is displayed. Choose either **Open** or **Save**.
- If you choose **Open**, the tabular report is displayed in the same browser window or a new browser window, depending on your browser.
- If you choose **Save**, you are prompted to choose a location where to save the file. The file can be opened with any spreadsheet program.
- To print the report, click the **Print** icon in the task bar.

## Viewing Reports

- [Report Types, page 10-22](#)
- [Report Content, page 10-24](#)

## Report Types

Access the following:

- [System Wide Reports, page 10-23](#)
- [Location Reports, page 10-23](#)
- [Service Engine Reports, page 10-23](#)

## System Wide Reports

To access the system-wide reports:

- 
- Step 1** Click the **Home** link in the upper-right corner of the CDSM browser window.
  - Step 2** To change the report parameters for the System-Wide Bandwidth Served or System-Wide Bandwidth Efficiency Gain graphs, click **View Detailed Report**.
  - Step 3** Click the **Streaming Sessions** link to open the System-Wide Streaming Sessions page.



### Note

Each report has a new data point every five minutes. The last data point (or last few data points if the System.datafeed.pollRate is greater than five minutes) for system-wide reports and location-based reports may fluctuate until the data point time interval has passed. The System.datafeed.pollRate determines how often the system polls each SE for data. If the poll rate is one minute, five polling values contribute to the data point in the report. The last data points in the system-wide reports are dynamic because they may not have all the polling values yet.

The System-monitoring.collectRate is the rate at which the SE collects and reports statistics data to the CDSM. At each collection period, the SE collects bandwidth values from each protocol engine and reports that information to the CDSM.

To change the System.datafeed.pollRate and System.monitoring.collectRate settings, see the [“System Properties” section on page 9-7](#)



### Note

If the report states, “Insufficient data. Please make sure NTP is configured on the SE.” Be sure NTP is configured for each device that is contributing data to the report. See the [“Configuring NTP” section on page 5-79](#) for more information.

## Location Reports

To access reports covering activity for a location:

- 
- Step 1** Choose **Devices > Locations**. The Location Table page is displayed.
  - Step 2** Click the **Edit** icon next to the location name. The Location page is displayed.
  - Step 3** Choose **Statistics** and choose one of the following reports: **Bandwidth Served**, **Bandwidth Efficiency Gain**, or **Streaming Sessions**.

## Service Engine Reports

To access reports covering activity for an SE:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the device name. The Devices home page is displayed.

**Step 3** Choose **Monitoring > Statistics** and choose one of the following reports:

- **Bandwidth Served**
- **Bandwidth Efficiency Gain**
- **Streaming Sessions**

The reports are described in the following sections.

Additional tips:

- To export the report to a CSV (comma-separated value) file, click the **Export** icon in the task bar. A dialog box is displayed. Choose either **Open** or **Save**.
- If you choose **Open**, depending on your browser, the tabular report is displayed in either a new browser window or the same browser window.
- If you choose **Save**, you are prompted to choose a location where to save the file. The file can be opened with any spreadsheet program.
- To print the report, click the **Print** icon in the task bar.

## Report Content

There are three reports available for monitoring traffic in graphical or tabular format:

- [Bandwidth Served, page 10-24](#)
- [Bandwidth Efficiency Gain, page 10-25](#)
- [Streaming Sessions, page 10-26](#)

### Bandwidth Served

The Bandwidth Served report provides information about the total outgoing bandwidth of all the protocol engines on an SE, or if you are viewing the system-wide report, all the protocol engines on all the SEs in the system. The Bandwidth Served report also provides a table with the Maximum Value, Average Value, and License Limit. The Maximum Value is the maximum rate (in bits per second) achieved for the specified content type. The *Average Value* is the average rate (in bits per second) for the specified content type during the specified period of time. The License Limit does not currently apply to the Enterprise CDS software.



#### Note

The Bandwidth Served report displays information based on clients that have completed their downloads. Clients that are in the process of downloading when the report is generated are not reflected in the Bandwidth Served report.

To change the report settings and view the changes, navigate to the page using the instructions provided at the beginning of the [“Viewing Reports” section on page 10-22](#).

[Table 10-12](#) describes the report settings.

**Table 10-12 Bandwidth Served Report Settings**

| Field                  | Description                                                                                                                                                                                                                                   |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server                 | The options are HTTP, Windows Media, Movie Streamer, or Flash Media Streaming. Check the check boxes next to the protocol engines you want to include in the graph.                                                                           |
| Chart Style            | The options are line or area.                                                                                                                                                                                                                 |
| Chart Size             | The chart display size choices are small, medium, or large.                                                                                                                                                                                   |
| Aggregation Method     | For system-wide and location reports only. Choices are sum or average, where sum gives you the sum total of all bandwidth served in the system or location, and average divides the sum total by the number of SEs in the system or location. |
| Include Child Location | For location report only. If checked, all child locations are included in the report.                                                                                                                                                         |
| Time Frame             | The time frame options are last hour, last day, last week, last month, or custom.                                                                                                                                                             |
| Time Zone              | The time zone choices are SE local time, CDSM local time, or UTC.                                                                                                                                                                             |
| Custom Date Range      | The custom date range is used when Time Frame is set to custom. Enter the dates, beginning and end, for the chart in the mm/dd/yyyy format, or choose the dates by using the calendar icons.                                                  |

**Tip**

Set the Chart Style to medium to see the legend and timeline across the bottom.

## Bandwidth Efficiency Gain

After an SE has been in use for some time and has collected statistics, the Bandwidth Efficiency Gain report can demonstrate the value of the SE in terms of bandwidth savings. The bandwidth efficiency is calculated by subtracting the bandwidth in from the bandwidth out, providing the bandwidth saved from serving content from the SE (cache hit, pre-positioned content, or splitting of live streams).

[Table 10-13](#) describes the report settings.

**Table 10-13 Bandwidth Efficiency Gain Report Settings**

| Field                  | Description                                                                                                                                                                                                                                   |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Series                 | The series options are In, Out, and Efficiency Gain. The In option creates a graph for bandwidth used for incoming data. The Out option is for outgoing data, and Efficiency Gain is the combination of the two.                              |
| Chart Size             | The chart display size choices are small, medium, or large.                                                                                                                                                                                   |
| Aggregation Method     | For system-wide and location reports only. Choices are sum or average, where sum gives you the sum total of all bandwidth served in the system or location, and average divides the sum total by the number of SEs in the system or location. |
| Include Child Location | For location report only. If checked, all child locations are included in the report.                                                                                                                                                         |

**Table 10-13** *Bandwidth Efficiency Gain Report Settings (continued)*

| Field             | Description                                                                                                                                                                                  |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Frame        | The time frame options are last hour, last day, last week, last month, or custom.                                                                                                            |
| Time Zone         | The time zone choices are SE local time, CDSM local time, or UTC.                                                                                                                            |
| Custom Date Range | The custom date range is used when Time Frame is set to custom. Enter the dates, beginning and end, for the chart in the mm/dd/yyyy format, or choose the dates by using the calendar icons. |

**Tip**

Set the Chart Size to medium to see the legend and timeline across the bottom.

## Streaming Sessions

The Streaming Sessions report lists the total number of streaming sessions in progress at the collection time. It allows you to plan for future hardware provisioning and licensing requirements based on utilization data. [Table 10-14](#) describes the report settings.

**Table 10-14** *Streaming Sessions Report Settings*

| Field                  | Description                                                                                                                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server                 | The options are Windows Media unicast, Windows Media multicast, Movie Streamer unicast, or Flash Media unicast. Check the check boxes next to the streaming types you want to include in the graph.                                       |
| Chart Size             | The chart display size choices are small, medium, or large.<br><b>Tip</b> Set the Chart Size to medium to see the legend and timeline across the bottom.                                                                                  |
| Aggregation Method     | For system-wide and location reports only. Choices are sum or average, where sum gives you the sum total of all bytes served in the system or location, and average divides the sum total by the number of SEs in the system or location. |
| Include Child Location | For location report only. If checked, all child locations are included in the report.                                                                                                                                                     |
| Time Frame             | The time frame options are last hour, last day, last week, last month, or custom.                                                                                                                                                         |
| Time Zone              | The time zone choices are SE local time, CDSM local time, or UTC.                                                                                                                                                                         |
| Custom Date Range      | The custom date range is used when Time Frame is set to custom. Enter the dates, beginning and end, for the chart in the mm/dd/yyyy format, or choose the dates by using the calendar icons.                                              |

**Note**

Streaming Sessions statistics report for Movie Streamer is only available for unicast. When a client is joining a multicast group for multicast streaming, ECDS Movie Streamer only knows that a client is downloading the SDP file, but no information is exchanged between the client and Movie Streamer on the streaming data session; therefore there are no session statistics for multicast Movie Streamer sessions.



# Delivery Service Monitoring

This section describes the following topics:

- [Delivery Services Table, page 10-27](#)
- [Replication Status for a Delivery Service, page 10-30](#)

## Delivery Services Table

The Delivery Services Table page lists all delivery services on the system and displays the replication status information for each delivery service. This display summarizes the replication status of all SEs associated with a specific delivery service in a given state.

[Table 10-15](#) describes the icons for the delivery service table. To view or modify the configuration of a delivery service, click the **Edit** icon next to the delivery service name. To create a new delivery service, click the **Create New** icon in the task bar.

**Table 10-15** *Delivery Service Table Icons*

| Icon                                                                                | Function                                                                                                            |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
|    | Creates a new delivery service.                                                                                     |
|  | Edits a delivery service.                                                                                           |
|  | Creates a filtered table. Filter the delivery service by the delivery service name and content origin.              |
|  | Views all delivery services. Click this icon to view all delivery services after you have created a filtered table. |
|  | Refreshes the table.                                                                                                |
|  | Prints the current window.                                                                                          |

For more information, see the [“Devices, Services, and Other Tables” section on page 3-7](#).

To view system-wide replication status for each delivery service:

- 
- Step 1** Choose **Services > Delivery Services** to display the Delivery Services Table page, as shown in [Figure 10-7](#).

Figure 10-7 Delivery Services Table Page

| Delivery Service | Type    | Content Origin | Status | State | Replication Status |
|------------------|---------|----------------|--------|-------|--------------------|
| 100kbs           | Content | 100kbsfiles    |        | N/A   | N/A                |
| 1mbs             | Content | 1mbs           |        | N/A   | N/A                |
| 1mbs100          | Content | 1mbs100file    |        | N/A   | N/A                |
| 375mbs100wmv     | Content | 375mbs100files |        | N/A   | N/A                |
| 375mbs           | Content | 375Mbs         |        | N/A   | N/A                |
| 429mbfile        | Content | 429mbfile      |        | N/A   | No Status Reported |
| 4gbfile          | Content | 4GBfile        |        | N/A   | N/A                |
| 8kbfile          | Content | 8kfiles        |        | N/A   | N/A                |
| 8kbs             | Content | 8kb            |        | N/A   | No Status Reported |
| allfiles         | Content | allfiles       |        | N/A   | N/A                |

**Step 2** View the replication status information for each delivery service. [Table 10-16](#) describes the status information that is displayed on this page.

Table 10-16 System-Wide Replication Status by Delivery Service

| Column Heading   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delivery Service | Name of the delivery service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Type             | Type of delivery service. The delivery service types are Live and Content.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Content Origin   | Name of the Content Origin assigned to the delivery service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Status           | <p>Graphical display indicating acquisition, replication, and device errors. Status lights represent the highest level of errors encountered:</p> <ul style="list-style-type: none"> <li>Green—No errors encountered.</li> <li>Yellow—Only minor errors encountered.</li> <li>Red—At least one critical error encountered, such as an acquisition failure, a content replication failure, or a failed or nonresponsive SE.</li> </ul> <p>For details of the errors, click the status light for a particular delivery service, which takes you to the Replication Status for Delivery Service page. (See <a href="#">Table 10-17</a> for a description of status errors and their corresponding status lights.)</p> |

**Table 10-16 System-Wide Replication Status by Delivery Service (continued)**

| Column Heading | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| State          | <p>State of the delivery service. States are reported for the Content Acquirer and for receiver SEs. (See <a href="#">Table 10-18</a> for a definition of the different delivery service states.)</p> <p>The state is also a link to the Replication Status for Delivery Service page that provides a more detailed view of the replication status for the delivery service. (See <a href="#">Figure 10-8</a>.)</p>                                                                                                             |
| Manifest State | <p>State of the Manifest file. States reported are as follows:</p> <ul style="list-style-type: none"> <li>• Fetching—The Manifest file is being fetched.</li> <li>• Fail Fetching—The Manifest file has failed to be fetched.</li> <li>• Parsing—The Manifest file is being parsed.</li> <li>• Fail Parsing—The Manifest file has failed to be parsed.</li> <li>• Completed—The Manifest file was successfully fetched and parsed.</li> <li>• No Status Reported—Content Acquirer is in a Pending or Disabled state.</li> </ul> |

[Table 10-17](#) describes the status errors and their corresponding status lights.

**Table 10-17 Delivery Service Status Errors**

| Status Light | Error                                        | Description                                                                                                                      |
|--------------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Yellow       | Manifest retrieval error                     | The Content Acquirer cannot retrieve the Manifest file for one or two consecutive attempts.                                      |
| Red          | Manifest retrieval error                     | The Content Acquirer cannot retrieve the Manifest file for three consecutive attempts.                                           |
| Red          | Manifest syntax error                        | The Content Acquirer fails to parse the Manifest file.                                                                           |
| Red          | Crawl job processing error                   | The Content Acquirer encounters problems while crawling for content.                                                             |
| Red          | Acquisition or content replication error     | The SE fails to obtain the content.                                                                                              |
| Red          | Disk quota exceeded error                    | The SE cannot store or process the content because there is no more disk space available.                                        |
| Yellow       | Replication status update error              | Content replication failed for one or two consecutive attempts.                                                                  |
| Red          | Replication status update error              | Content replication failed for three or more consecutive attempts.                                                               |
| Red          | SE unreachable error                         | The SE is offline or the SE has not responded to replication status requests for three consecutive polling periods.              |
| Red          | Root SE failover                             | The Content Acquirer has failed over to a temporary Content Acquirer. Receiver SEs have not identified a valid Content Acquirer. |
| Red          | Receiver SE device or delivery service error | Receiver SE is not reporting replication status or any other content replication problem.                                        |

Table 10-18 defines the different delivery service states.

**Table 10-18 Delivery Service States in Replication Status**

| State      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Completed  | <p>All receiver SEs are in the Completed state, and the Content Acquirer is in the Completed, Re-checking Content, Retrieving Manifest, or Processing Manifest state. (See <a href="#">Table 10-21 on page 10-32</a> for a description of SE states.)</p> <p>When the Content Acquirer in the Re-checking Content state determines that new content needs to be acquired, the delivery service state changes to In Process.</p>                    |
| In Process | <p>In Process can mean:</p> <ul style="list-style-type: none"> <li>Content Acquirer is in the Retrieving Manifest, Processing Manifest, Acquiring Content, or Re-checking Content state.</li> <li>Any receiver SE is in the Pending Update from Content Acquirer, Replicating, or Recovering from Failure state.</li> <li>Content Acquirer has failed and receiver SEs are still reporting status.</li> </ul>                                      |
| Failed     | <p>Failed can mean:</p> <ul style="list-style-type: none"> <li>Acquisition or content replication error has occurred. (See <a href="#">Table 10-17 on page 10-29</a>.)</li> <li>SE has gone offline or has not reported status in three consecutive polling periods.</li> <li>Delivery service has more than one Content Acquirer</li> <li>Delivery service has no Content Acquirer, but has receiver SEs reporting replication status.</li> </ul> |

## Replication Status for a Delivery Service

To view the replication status for a delivery service, you can either click the alarm light or **Replication Status** link in the Delivery Services Table page, or click the **Replication Status** option from the Delivery Service left-panel menu.

- [Content Replication Status by Delivery Service, page 10-33](#)
- [Content Replication Status by Device, page 10-35](#)

Figure 10-8 shows the Replication Status page for a delivery service. The Replication Status page is refreshed automatically every 15 seconds.

**Figure 10-8** Delivery Service Replication Status Page

**Replication Status for Delivery Service, fms**

**Acquisition Status**

User Selected Content Acquirer: GE-612-2      Current Content Acquirer: GE-612-2

Disk Quota Used: 456.754 MB / 9.766 GB      Status: Completed

Manifest Last Modified Time: Wed Mar 04 09:33:11 GMT 2009      Manifest Last Checked Time: Tue May 05 16:35:52 GMT 2009

**View Detailed Replication Status**

Get Detailed Status using Search Criteria

**View Detailed Replication Status for Delivery Service by Device**

Get  content items using Search Criteria  for Selected Device

**Devices Assigned to Delivery Service, fms** Rows: ALL

| Device   | Type     | Status | State     | Progress in % | Last Report Time    | File Count |            |        |       |
|----------|----------|--------|-----------|---------------|---------------------|------------|------------|--------|-------|
|          |          |        |           |               |                     | Completed  | In Process | Failed | Total |
| GE-612-2 | Acquirer |        | Completed | 100.00        | 16:36:44 05-05-2009 | 7          | 0          | 0      | 7     |
| GE-612-6 | Receiver |        | Completed | 100.00        | 16:36:50 05-05-2009 | 7          | 0          | 0      | 7     |
| GE-612-7 | Receiver |        | Completed | 100.00        | 16:36:33 05-05-2009 | 7          | 0          | 0      | 7     |

<< Page 1 >> Showing 1-3 of 3 Devices

This page also allows you to:

- See a detailed view of replication status using search criteria. (See the “[Content Replication Status by Delivery Service](#)” section on page 10-33.)
- Query the replication status of content items (by pattern) for a selected SE in the delivery service. (See the “[Content Replication Status by Device](#)” section on page 10-35.)

The information on the Replication Status page is refreshed approximately every ten seconds.

[Table 10-19](#) describes the fields in Acquisition Status section of this page.

**Table 10-19** Replication Status for a Delivery Service

| Field                          | Description                                                                                                                                                                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Selected Content Acquirer | Name of the user-selected Content Acquirer.                                                                                                                                                                                                                       |
| Current Content Acquirer       | Name of the current Content Acquirer. The current Content Acquirer is the same as the user-selected Content Acquirer as long as the user-selected one is active; if it fails for any reason, the temporary Content Acquirer becomes the current Content Acquirer. |
| Disk Quota Used                | Amount of available disk space used for the delivery service.                                                                                                                                                                                                     |
| Status                         | State of the Content Acquirer. (For a description of Content Acquirer states, see <a href="#">Table 10-21</a> .)                                                                                                                                                  |
| Manifest Last Modified Time    | Time when the Manifest file was last saved, as recorded on the SE.                                                                                                                                                                                                |
| Manifest Last Checked Time     | Time when the Content Acquirer last checked the Manifest file for changes.                                                                                                                                                                                        |

[Table 10-20](#) describes the information about the devices in this delivery service shown at the bottom of the Replication Status page.

**Table 10-20**      *Replication Status for Devices Assigned to a Delivery Service*

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device            | Name of the SE assigned to the delivery service.                                                                                                                                                                                                                                                                                                                                                                               |
| Type              | Type of SE: Acquirer, Receiver, or Temporary Acquirer.                                                                                                                                                                                                                                                                                                                                                                         |
| Status            | Graphical display indicating acquisition, replication, and device errors. Status lights represent the highest level of errors encountered: <ul style="list-style-type: none"> <li>Green—No errors encountered.</li> <li>Yellow—Only minor errors encountered.</li> <li>Red—At least one critical error encountered, such as an acquisition failure, a content replication failure, or a failed or nonresponsive SE.</li> </ul> |
| State             | State of either the Content Acquirer or receiver SEs. (See <a href="#">Table 10-21</a> for a description of SE states.)                                                                                                                                                                                                                                                                                                        |
| Progress          | Replication progress (in percent). The interval between progress updates is configurable. See the “ <a href="#">System Properties</a> ” section on <a href="#">page 9-7</a> of <a href="#">Chapter 9, “Configuring the System.”</a>                                                                                                                                                                                            |
| Last Report Time  | Time when the last report from the SE was received by the CDSM. This time stamp uses the CDSM clock.                                                                                                                                                                                                                                                                                                                           |
| <b>File Count</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Completed         | Number of files that the SE has successfully acquired or received.                                                                                                                                                                                                                                                                                                                                                             |
| In Process        | Number of new files to be acquired or replicated. Includes only files for which no acquisition or replication attempts have previously been made.                                                                                                                                                                                                                                                                              |
| Failed            | For the Content Acquirer: Number of files that failed to be acquired in at least one attempt.<br><br>For receiver SEs: Number of files that failed to be replicated in at least one attempt.<br><br><b>Note</b> The failure count for the receiver SE has no relationship to the failure count for the Content Acquirer. If the Content Acquirer fails to replicate an item, the receiver counts this item as “In Process.”    |
| Total             | Total number of Completed, In Process, and Failed files.                                                                                                                                                                                                                                                                                                                                                                       |

[Table 10-21](#) describes the states of the Content Acquirer or receiver SE.

**Table 10-21**      *Device States*

| State                   | Description                                                                                                              |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Content Acquirer</b> |                                                                                                                          |
| Retrieving Manifest     | The Content Acquirer is retrieving the Manifest file from the origin server or rechecking the Manifest file for changes. |
| Processing Manifest     | The Content Acquirer has retrieved the Manifest file and is parsing it.                                                  |

**Table 10-21**     *Device States (continued)*

| State                        | Description                                                                                                                                                                                                                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Acquiring Content            | The Content Acquirer has processed the Manifest file and is crawling or fetching content.                                                                                                                                                                                                                       |
| Re-checking Content          | The Content Acquirer is checking the content or crawl job freshness.                                                                                                                                                                                                                                            |
| No Status Reported           | No Status Reported can mean: <ul style="list-style-type: none"> <li>• The Content Acquirer is unreachable for three consecutive polling periods.</li> <li>• The Content Acquirer is offline.</li> <li>• The CDSM has recently restarted and has not yet received a report from the Content Acquirer.</li> </ul> |
| Completed                    | The Content Acquirer is not in the Retrieving Manifest, Processing Manifest, Acquiring Content, Re-checking Content, or No Status Reported state.                                                                                                                                                               |
| <b>Receiver SE</b>           |                                                                                                                                                                                                                                                                                                                 |
| Pending Update from Acquirer | The receiver SE is not synchronized with the Content Acquirer.                                                                                                                                                                                                                                                  |
| Replicating                  | The receiver SE is synchronized with the Content Acquirer and is replicating content.                                                                                                                                                                                                                           |
| Completed                    | The receiver SE has finished replicating all the content with no errors.                                                                                                                                                                                                                                        |
| Recovering from Failure      | The receiver SE has not identified the Content Acquirer. This state occurs during a failover from the Content Acquirer to a temporary Content Acquirer.                                                                                                                                                         |
| No Status Reported           | No Status Reported can mean: <ul style="list-style-type: none"> <li>• Receiver SE is unreachable for three consecutive polling periods.</li> <li>• Receiver SE is offline.</li> <li>• CDSM has recently restarted and has not yet received a report from the receiver Service Engine.</li> </ul>                |

## Content Replication Status by Delivery Service

In the View Detailed Replication Status section of the Replication Status page, enter a search string in the **Get Detailed Status Using** field and click **Go**.



### Tip

For help with search string characters, click **Search Criteria**.

Use an asterisk (\*) to match one or more characters, or a question mark (?) to match only a single character. The criteria are matched against the relative *cdn-url* attribute specified in the <item> tag in the Manifest file. We recommend that you start the search criteria by specifying wildcards such as \*.htm or \*.clip.mpeg.

Figure 10-9 shows the results of a detailed status search for a delivery service.

**Figure 10-9**      *Replication Status for Searched Content Items in a Delivery Service*

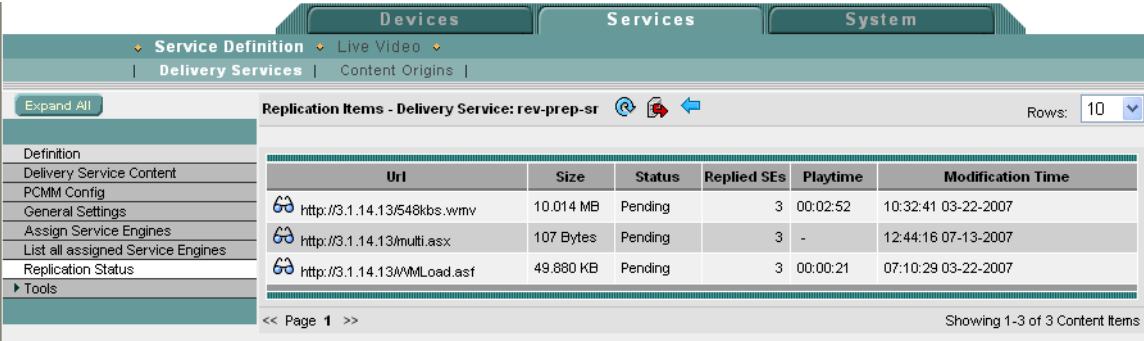


Table 10-22 describes the information displayed for the replication items.

**Table 10-22**      *Replication Status of Items for a Delivery Service*

| Column Heading    | Description                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Url               | URL of the origin server that stores the content.                                                                                                                  |
| Size              | Size of the file to be acquired or crawled.                                                                                                                        |
| Status            | Status of replication of content in the delivery service. The status is shown as Complete if replication is completed on all SEs assigned to the delivery service. |
| Replied SEs       | Number of SEs that have replicated this item.                                                                                                                      |
| Playtime          | Duration of playback of the file.                                                                                                                                  |
| Modification Time | Timestamp of the earliest update for that delivery service from an active SE.                                                                                      |



**Note**

When you click the **Force replication information refresh** icon in the task bar, the system displays a dialog box asking you to confirm whether you want to refetch the information from SEs assigned to this delivery service. To continue with the refresh process, click **OK**. You are notified that the request has been queued and are asked to check back later.

To return to the previous page, click the **Back** icon in the task bar.

To get detailed information about the replication status of the content item, click the **View** icon (eyeglasses) next to the URL. Detailed replication information is displayed (Figure 10-10). This page provides details on the replication status of the content item for every SE in the delivery service.



**Figure 10-10** Replication Status for Searched Content Items in a Delivery Service—Detail

| SE        | Size      | Status   | Playtime | Modification Time   |
|-----------|-----------|----------|----------|---------------------|
| CC-612-4  | 10.014 MB | Complete | 00:02:52 | 10:32:41 03-22-2007 |
| CC-612-5  | 10.014 MB | Complete | 00:02:52 | 10:32:41 03-22-2007 |
| CC-7326-1 | 10.014 MB | Complete | 00:02:52 | 10:32:41 03-22-2007 |



**Note** The Replication Item page is specifically designed to limit listings to 5000 objects for scalability reasons. These are system limits and not specifically enforced for replication status reporting.

Table 10-23 describes the information on this page.

**Table 10-23** Replication Status of an Item for All SEs in a Delivery Service

| Column Heading    | Description                                                                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| SE                | Name of the SE to which the item has been replicated.                                                                                                   |
| Size              | Size of the file to be acquired or crawled.                                                                                                             |
| Status            | Status of the replication of the content on the SE. Status is shown as Complete if replication is complete on all SEs assigned to the delivery service. |
| Playtime          | Duration of playback of the file.                                                                                                                       |
| Modification Time | Timestamp of the latest update for the content item as recorded on the origin server.                                                                   |

To return to the previous page, click the **Back** icon in the task bar.

## Content Replication Status by Device

Queries to determine the detailed replication status of a content item trigger extensive CPU cycles and high consumption of memory, because all the SEs assigned to a delivery service need to be polled, and the retrieved replication status is cached in the memory of the CDSM. This results in performance degradation. To optimize the use of memory resources without compromising the need to obtain detailed replication status of a particular content item, you can choose an SE assigned to a delivery service and generate a query.

To view the detailed replication status for a delivery service by device:

- Step 1** From the Replication Status page, in the Devices Assigned to Delivery Service section (see Figure 10-8), click the radio button next to the name of the device that you want to view.
- Step 2** In the View Detailed Replication Status for Delivery Service by Device section:
  - a. Choose content items from the **Get** drop-down list:
    - all

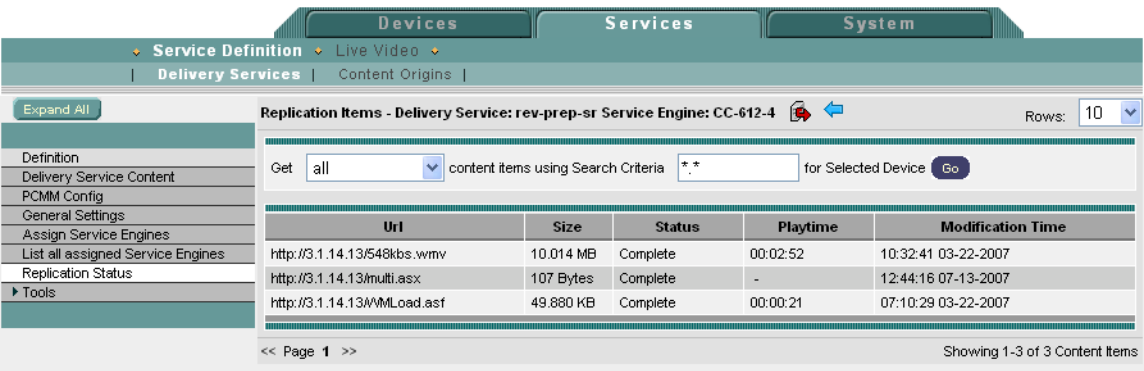
- replicated
- nonreplicated
- b. In the **Content Items Using** field, enter a string that specifies the type of content items that you want displayed and click **Go**.



**Note** Use an asterisk (\*) to match one or more characters, or a question mark (?) to match only a single character.

The Replication Items page for the selected device is displayed, as shown in [Figure 10-11](#).

**Figure 10-11** Replication Items for a Selected Device



[Table 10-24](#) describes the fields displayed in this page.

**Table 10-24** Replication Status of Items for a Delivery Service by Device

| Column Heading    | Description                                                                          |
|-------------------|--------------------------------------------------------------------------------------|
| Url               | URL of the origin server that stores the content.                                    |
| Size              | Size of the file to be acquired or crawled.                                          |
| Status            | Status of replication of content for the selected SE.                                |
| Playtime          | Duration of playback of the file.                                                    |
| Modification Time | Timestamp of the latest update to the content item as recorded on the origin server. |



**Note** When you click the **Force replication information refresh** icon in the task bar, the system displays a dialog box asking you to confirm whether you want to refetch the information from SEs assigned to this delivery service. To continue with the refresh process, click **OK**. You are notified that the request has been queued and are asked to check back later.

**Step 3** To refine your search from this window:

- a. Make a choice from the **Get** drop-down list.
- b. Enter a search string in the **Content Items Using** field.
- c. Click **Go** to retrieve the specified items.

**Step 4** To return to the Replication Status page, click the **Back** icon in the task bar.

## Viewing Statistics

The Statistics pages track system-wide delivery, replication, and routing traffic in the ECDS. You can view statistics on delivery traffic (Movie Streamer, Windows Media, HTTP, and Flash Media) listed by SE or device group. The Routing Statistics page lists client requests and redirects. The Replication Statistics page lists the replication status for all SEs in the ECDS, and provides a drill-down to all delivery services for a chosen SE, and all content items associated with that delivery service.

This section contains the following procedures:

- [Viewing Service Engines and Device Group Statistics, page 10-37](#)
- [Viewing Routing Statistics, page 10-39](#)
- [Viewing Replication States, page 10-39](#)

## Viewing Service Engines and Device Group Statistics

To view the statistics for all SEs or all device groups:

- Step 1** Choose **Devices > Statistics**. The Statistics page is displayed.
- Step 2** Choose **Service Engines** or **Device Groups**, and then choose one of the following content delivery types:
- **Movie Streamer**
  - **HTTP**
  - **Windows Media**
  - **Flash Media**

[Table 10-25](#) describes the icons on the Statistics pages.

**Table 10-25 Statistics Icons**

| Icon                                                                                | Function                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Update application statistics. The statistics are updated at a configurable time interval, which is set in the System Configuration page (System.monitoring.collectRate). See the <a href="#">“Configuring System Settings” section on page 9-7</a> . To see the latest statistics immediately, without waiting for the time interval to elapse, click this icon. |
|  | Export a table to a comma-separated value (CSV) file.                                                                                                                                                                                                                                                                                                             |
|  | Refresh the table                                                                                                                                                                                                                                                                                                                                                 |
|  | Print the current window.                                                                                                                                                                                                                                                                                                                                         |

Table 10-26 describes each statistic for each content delivery type.

**Table 10-26 Service Engine and Device Group Statistics**

| Statistic             | Description                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Movie Streamer</b> |                                                                                                                                                        |
| Bandwidth In          | Current bandwidth used for input by the Movie Streamer in bits per second.                                                                             |
| Bandwidth Out         | Current bandwidth used for output by the Movie Streamer in bits per second.                                                                            |
| Bandwidth In          | Total bandwidth, in bits per second, received by the Movie Streamer since it was started.                                                              |
| Bandwidth Out         | Total bandwidth, in bits per second, transmitted by the Movie Streamer since it was started.                                                           |
| Packets In            | Total packets received by the Movie Streamer since it was started.                                                                                     |
| Packets Out           | Total packets transmitted by the Movie Streamer since it was started.                                                                                  |
| RTSP Connections      | Number of clients currently connected over RTSP.                                                                                                       |
| RTP Connections       | Number of clients connected since startup.                                                                                                             |
| Updated               | Timestamp indicating when the statistics were updated.                                                                                                 |
| <b>HTTP</b>           |                                                                                                                                                        |
| Requests/Sec          | Number of requests per second.                                                                                                                         |
| Bytes/Sec             | Number of bytes per second.                                                                                                                            |
| Request Latency       | Average number of seconds per HTTP request.                                                                                                            |
| Hit Rate              | Average number (as a percentage) of content items successfully served per minute from the cache of the SE or from all the SEs in the device group.     |
| Updated               | Timestamp indicating when the statistics were updated.                                                                                                 |
| <b>Windows Media</b>  |                                                                                                                                                        |
| Concurrent Requests   | Total number of simultaneous requests the Windows Media Streaming Engine has served.                                                                   |
| Bandwidth             | Current bandwidth, in bits per second, that is used for output.                                                                                        |
| Cache Hit Rate        | Average number (as a percentage) of content items successfully served per minute from the cache of the SE or from all the SEs in the device group.     |
| Updated               | Timestamp indicating when the statistics were updated.                                                                                                 |
| <b>Flash Media</b>    |                                                                                                                                                        |
| Byte/Sec              | Total number of bytes per second served.                                                                                                               |
| All Connections       | Number of clients currently connected.                                                                                                                 |
| Cache Hit Rate        | Average number (as a percentage) of content items successfully served per minute from the cache of the SE or from all the SEs in the delivery service. |
| Updated               | Timestamp indicating when the statistics were updated.                                                                                                 |

## Viewing Routing Statistics

To view the routing statistics for SRs:

**Step 1** Choose **Devices > Statistics > Routing Statistics**.

**Step 2** Choose one of the following options:

- **Routing Requests**
- **Routing Redirects**

[Table 10-25](#) describes the icons on the Routing Statistics pages. [Table 10-27](#) describes each routing statistic.

**Table 10-27 Service Router Statistics**

| Statistic                | Description                                               |
|--------------------------|-----------------------------------------------------------|
| <b>Routing Requests</b>  |                                                           |
| Total Requests           | Total number of content requests received from clients.   |
| HTTP Requests            | Number of ASX and traditional HTTP web requests received. |
| RTSP Requests            | Number of RTSP requests received.                         |
| RTMP Requests            | Number of RTMP requests received.                         |
| Updated                  | Timestamp indicating when the statistics were updated.    |
| <b>Routing Redirects</b> |                                                           |
| Total Requests           | Total number of content requests received from clients.   |
| Reqs Redirected          | Total number of redirected client requests.               |
| Reqs Not Redirected      | Total number of client requests not redirected.           |
| Updated                  | Timestamp indicating when the statistics were updated.    |

## Viewing Replication States

To view system-wide replication states by device:

**Step 1** Choose **Devices > Statistics > Replication Status**. The replication states for all SEs in the ECDS are displayed.

[Table 10-28](#) describes the status information displayed on this page.

**Table 10-28**     *Device Replication Status Page*

| Column Heading         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device                 | Name of the SE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Status                 | Graphical display indicating acquisition, replication, and device errors. Status lights represent the highest level of errors encountered: <ul style="list-style-type: none"> <li>Green—No errors encountered.</li> <li>Yellow—Only minor errors encountered.</li> <li>Red—At least one critical error encountered, such as an acquisition failure, a content replication failure, or a failed or nonresponsive SE.</li> </ul> (See <a href="#">Table 10-17</a> for a description of status errors and their corresponding status lights.) |
| Delivery Service Count | Number of delivery services reporting SEs in a particular state. (See <a href="#">Table 10-21</a> for a description of SE states.)                                                                                                                                                                                                                                                                                                                                                                                                         |
| Completed              | Number of delivery services reporting this SE in a Completed state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| In Process             | In Process can mean: <ul style="list-style-type: none"> <li>Number of delivery services reporting this SE (as a Content Acquirer) in the Retrieving Manifest, Processing Manifest, Acquiring Content, or Re-checking Content state.</li> <li>Number of delivery services reporting this SE (as a receiver SE) in the Pending Update from Acquirer, Replicating, or Recovering from Failure state.</li> </ul>                                                                                                                               |
| Failed                 | Number of delivery services reporting this SE in the Failed or Failed Update state.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Unknown                | Number of delivery services reporting this SE in the No Status Reported state.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Step 2** To view the statistics on the delivery services associated with this SE, click **View** (the eyeglasses icon) next to the SE.

The Replication Status for each delivery service that uses the SE to deliver content is displayed. The first column in this table lists the delivery service that uses the SE, the columns that follow list information about the SE's function in the delivery service. For a description of the subsequent columns, see [Table 10-20 on page 10-32](#).

**Step 3** To view replication details for the selected delivery service, click the radio button next to the delivery service name.

To view the forwarding path for this delivery service, click **View** (the eyeglasses icon) next to the delivery service. After you are finished viewing the forwarding path, choose **Replication Status** to return to the Replication Status page.

**Step 4** From the **Get** drop-down list, choose the type of items to display

- all
- replicated
- non replicated

**Step 5** In the **Content Items Using** field, enter a regular expression (such as **\*.html**, **\*.mpg**, **\*.jpg**, or **\*.\***). Use an asterisk (\*) to match one or more characters, and a question mark (?) to match exactly one character.

- Step 6** To retrieve the specified items, click **Go**. The Replication Items for Delivery Service page is displayed. [Table 10-29](#) describes the fields displayed in this page.



**Note** The Replication Items for Delivery Service page is specifically designed to limit listings to 5000 objects for scalability reasons. These are system limits and are not specifically enforced for replication status reporting.

**Table 10-29** *Replication Status of Items for SEs in a Selected Delivery Service*

| Column Heading    | Description                                                                   |
|-------------------|-------------------------------------------------------------------------------|
| URL               | URL of the origin server that stores the content.                             |
| Size              | Size of the file to be acquired or crawled.                                   |
| Status            | Status of replication of content from the Content Acquirer.                   |
| Playtime          | Duration of playback of the file.                                             |
| Modification Time | Timestamp of the earliest update for that delivery service from an active SE. |

- Step 7** To further qualify your search, change the item type from the drop-down list, if you wish, or specify another file type (such as **\*.html**, **\*.mpg**, or **\*.jpg**) in the **Content Items Using** field. To retrieve the specified items, click **Go**.
- Step 8** To forcibly refetch the latest content replication information, click the **Force Replication Information Refresh** icon in the task bar. You are asked to confirm whether or not you wish to refetch the information from the SE assigned to the particular delivery service.
- Step 9** To continue with the refresh process, click **OK**. You are notified that your request has been sent and prompted to check back after a few minutes.
- Step 10** To return to the Replication Status page, click the **Back** button in the task bar.



**Tip** To view the SE forwarder path for a selected delivery service, click the **View** icon next to the name of the delivery service. To return to the Replication Status page, choose **Replication Status** in the left-panel menu.

## Managing Transaction Logs

Transaction logs allow administrators to view the traffic that has passed through the SE. Typical fields in the transaction log are the date and time when a request was made, the URL that was requested, whether it was a cache hit or a cache miss, the type of request, the number of bytes transferred, and the source IP address. For more information about configuring transaction log settings for SEs, see the [“Configuring Transaction Logging”](#) section on page 5-19.

This section describes the following topics:

- [Transaction Log Formats for Web Engine](#), page 10-42
- [Transaction Logging and NTLM Authentication](#), page 10-44

- [Usage Guidelines for Log Files, page 10-44](#)
- [Windows Media Transaction Logging, page 10-47](#)
- [Movie Streamer Transaction Log Fields, page 10-54](#)
- [Flash Media Streaming Transaction Log Fields, page 10-56](#)
- [Service Router Transaction Log Fields, page 10-63](#)

**Note**

Each transaction log includes a summary line as the last line in the transaction log, which includes a summary of all the requests that appear in the transaction log.

## Transaction Log Formats for Web Engine

The section describes the following different logging formats for Web Engine:

- [Extended Squid, page 10-42](#)
- [Apache, page 10-42](#)
- [Custom Format, page 10-43](#)

**Note**

Changing the time zone on an SE does not affect the log entry timestamps, only the log filename. The log entries always use UTC.

## Extended Squid

The Extended Squid format logs the same fields logged by the Squid-1.1 access log file format.

For details on the Squid-1.1 native log file format, see the Squid documentation “Frequently Asked Questions,” “Squid Log” section, access.log heading at:

<http://wiki.squid-cache.org/SquidFaq/FaqIndex>

The Extended Squid-style log file format is as follows:

Current-Time Time-to-Serve Client-IP Request-Desc/Status-Returned Bytes-Xferred Method URL  
MIME-Type

An Extended Squid-style log format example looks like this:

```
[21/May/2009:00:29:12 +0530] 952195 171.71.50.197 TCP_REFRESH_MISS/200 11120239 GET
http://7.9.0.3/1mbs_ai/1mbs1-100.wmv video/x-ms-wmv
```

## Apache

The Apache format is the Common Log File (CLF) format defined by the World Wide Web Consortium (W3C) working group. This format is compatible with many industry-standard log tools. For more information, see the W3C Common Log Format website:

<http://www.w3.org/Daemon/User/Config/Logging.html>.

The Apache-style log file format is as follows:

client-IP-address URI SE-IP-address bytes-sent object-size bytes-received method status time-received  
time-to-serve



An Apache-style log file format example looks like this:

```
171.71.50.197 http://spcdn-se612-5.se.sanity.spcdn.net/gmedia-0.4gb.wmv
SPCDN-SE612-5.spcdn.com 363704065 137 363710748 GET 200 [06/Nov/2007:00:25:32 +0530]
325033158
```

## Custom Format

The **transaction-logs format custom** command allows you to use a log format string to log additional fields that are not included in the predefined Extended Squid format or Apache CLF format. The log format string is a string that can contain the tokens listed in [Table 10-30](#) and that mimics the Apache log format string. The log format string can contain literal characters that are copied into the log file. Double backslashes (\\) can be used to represent a literal backslash, and a backslash followed by a single quote (\') can be used to represent a literal single quote. A literal double quote cannot be represented as part of the log format string. The control characters \t and \n can be used to represent a tab and a new line character, respectively.

The following command can be entered to generate the well-known Apache Combined Log Format:

**transaction-logs format custom "%t%r %>s %b"**

The following transaction log entry example is configured by using the preceding custom format string:

```
[11/Jan/2003:02:12:44 -0800] "GET http://www.cisco.com/swa/i/site_tour_link.gif HTTP/1.1" 200
3436
```

**Table 10-30 Custom Format Log Format String Values**

| Format Token | Value                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------------------------------|
| %a           | IP address of the requesting client.                                                                                |
| %A           | IP address of the SE.                                                                                               |
| %b           | Bytes sent, excluding HTTP headers.                                                                                 |
| %D           | Time consumed to serve the request in microseconds                                                                  |
| %h           | Remote host (IP address of the requesting client is logged).                                                        |
| %H           | Request protocol.                                                                                                   |
| %I           | Bytes received from the client.                                                                                     |
| %m           | Request method.                                                                                                     |
| %O           | Bytes sent to client, including the headers.                                                                        |
| %q           | Query string (which is preceded by a question mark (?) if a query string exists; otherwise, it is an empty string). |
| %r           | First line of the request.                                                                                          |
| %>s          | Status. The translog code always returns the HTTP response code for the request.                                    |
| %t           | Time in common log time format (or standard English format).                                                        |
| %T           | Time consumed to serve the request in seconds (a floating point number with 3 decimal places).                      |
| %U           | URL path requested, not including query strings.                                                                    |

**Table 10-30** Custom Format Log Format String Values (continued)

| Format Token | Value                                                                                                                                                                                                      |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %V           | Value of the host request header field reported if the host appeared in the request. If the host did not appear in the host request header, the IP address of the server specified in the URL is reported. |
| %X           | Connection status when the response is completed.                                                                                                                                                          |

## Transaction Logging and NTLM Authentication

If your device is configured for NT LAN Manager (NTLM) authentication and uses the Apache-style or Extended Squid-style format, you can record the Windows domain name and username in the “authenticated username” field of the transaction log. If the domain name is available, both the domain name and the username are recorded in the “authenticated username” field, in the form domain\username. If only the username is available, only the username is recorded in the “authenticated username” field. If neither a domain name nor a username is available, a “-” (hyphen) is recorded in the field.

## Usage Guidelines for Log Files

This section provides some guidelines for working with log files, and includes the following topics:

- [Working Logs, page 10-44](#)
- [Archive Working Log, page 10-45](#)
- [Exporting Log Files, page 10-45](#)

**Note**

Changing the time zone on an SE does not affect the log entry timestamps, only the log filename. The log entries always use UTC.

## Working Logs

Transaction logs are located in the /local/local/logs directory. Each component has one or more directories, depending on its configuration.

There is a working log file in each directory, which is a symbol link, linking to the current working log file.

The log files are logged to a working log on the local disk as follows:

- WMT logs are logged to a working log on the local disk in /local1/logs/export/working.log
- Movie Streamer logs are logged to a working log on the local disk in /local1/logs/movie-streamer/working.log
- Flash Media Streaming logs are logged to a working log on the local disk in /local1/logs/fms\_access/working.log and /local1/logs/fms\_authorization/working.log
- Service Router logs are logged to a working log on the local disk in the /local1/logs/service\_router/working.log
- Web Engine transaction logs are located in the /local1/logs/webengine\_apache, the /local1/logs/webengine\_clf, and the /local1/logs/webengine\_extsquid directories.

**Note**

For Movie Streamer, client requests that join the multicast group do not appear in the transaction log because multicast clients do not contact the server.

## Archive Working Log

You can specify the interval at which the working log should be cleared, when the interval occurs the data is moved to an archive log. The archive log files are located on the local disk in the /local1/logs/ directory.

The archiving of working logs can be configured to occur at a specified time interval and when the working log file reaches a specified size. If one of the criteria is met and at least one new message has been written to the working log, a log rotation occurs. If one of the criteria is met and no new messages have been written to the working log, a log rotation does not occur. You can specify the maximum number of old logs kept on disk.

Because multiple archive files are saved, the filename includes the timestamp when the file was archived. Because the files can be exported to an FTP/SFTP server, the filename also contains the IP address of the SE.

The archive filenames use this format:

modulename\_IPADDRESS\_YYYYMMDD\_HHMMSS\_file-generation-number.

For example, fms\_access\_10.74.61.130\_20070913\_080051\_065624\_00001 is the filename for the archive of the fms\_access log.

**Note**

The IP address used in the archived filename is not necessarily the primary interface of the SE. The transaction log function decides on which IP address to use in creating the archive name.

## Exporting Log Files

To facilitate the post-processing of cache log files, you can export transaction logs to an external host. This feature allows log files to be automatically exported by FTP to an external host at configurable intervals. The username and password used for FTP are configurable, as is the directory to which the log files are uploaded.

The log files automatically have a filename that uses the following format:

`<type>_<ipaddr>_<yyyymmdd_hhmmss>_<file_generation_number>`

- `<type>` represents the type of log file, with *selog* for cache logs such as HTTP, HTTPS, and FTP, and *mms\_export* for Windows Media Technologies (WMT) logs.
- `<ipaddr>` represents the SE IP address.
- `yyyymmdd_hhmmss` represents the date and time when the log was archived for export.
- `<file_generation_number>` represents the File Generation Number, which has a range from 00001 to 99999.

The following sections describe how to manage export log files:

- [Exporting Transaction Logs to External FTP Servers, page 10-46](#)
- [Restarting Export After Receiving a Permanent Error from the External FTP Server, page 10-46](#)
- [Exporting Transaction Logs to External SFTP Servers, page 10-46](#)

## Exporting Transaction Logs to External FTP Servers

To export transaction logs to an FTP server, you must first enable exporting of transaction logs and then configure the FTP or secure FTP (SFTP) server parameters. This feature can support up to four FTP servers. The following information is required for each target FTP server:

- Server IP address or the hostname

The SE translates the hostname with a DNS lookup and then stores the IP address in the configuration.

- FTP user login and user password
- Path of the directory where transferred files are written

Use a fully qualified path or a relative path for the user login. The user must have write permission to the directory.

You can also compress archived log files into gzip format before exporting them to external FTP servers. The compressed filename has a .gz extension. This compression feature uses less disk space than that required for noncompressed archived files on both the SE and the FTP export server and also requires less bandwidth during export because of the smaller size of the files to be exported.

For more information about exporting and archiving transaction logs, see the [“Configuring Transaction Logging” section on page 5-19](#) for SEs, and the [“Configuring Transaction Logs for the Service Router” section on page 6-7](#) for SRs.

To immediately have the transaction logs archived and exported following the next transaction, use the following commands:

```
SE# transaction-log force archive
SE# transaction-log force export
```

The **transaction-log force archive** command causes the transaction log to be archived to the SE hard disk following the next transaction. The **transaction-log force export** command causes the transaction log to be exported to the configured FTP server. The **transaction-log force** commands do not change the configured or default schedule for an archive or export of the transaction logs. The archive or export interval is restarted after the forced operation. If a scheduled archive or export job is in progress when the **transaction-log force** command is entered, the command has no effect.

## Restarting Export After Receiving a Permanent Error from the External FTP Server

When an FTP server returns a permanent error to the SE, the archive transaction logs are no longer exported to that server. You must re-enter the SE transaction log export parameters for the misconfigured server to clear the error condition.

A permanent error (Permanent Negative Completion Reply, RFC 959) occurs when the FTP command to the server cannot be accepted, and the action does not take place. Permanent errors can be caused by invalid user logins, invalid user passwords, and attempts to access directories with insufficient permissions or directories that do not exist.

## Exporting Transaction Logs to External SFTP Servers

You can also export transaction logs to a Secure File Transfer Protocol (SFTP) server. You must first enable the feature and configure the SFTP server parameters. The following information is required for each target SFTP server:

- SFTP server IP address or the hostname

The SE translates the hostname with a DNS lookup and then stores the IP address in the configuration.

- SFTP user login and user password
- Path of the directory where transferred files are written

Use a fully qualified path or a relative path for the user login. The user must have write permission to the directory.

To enable this feature, enter the **sshd allow-non-admin-users** command on the SE. If this feature is enabled, the output of the **show running-config EXEC** command shows that this feature is enabled on the SE.

## Windows Media Transaction Logging

The following formats are supported for Windows Media transaction logging:

- Standard Windows Media Services Version 4.1
- Extended Windows Media Services Version 4.1
- Standard Windows Media Services Version 9.0
- Extended Windows Media Services Version 9.0

The extended versions of the logging formats contain additional fields that are SE specific (For example, the SE-action field specifies a cache hit or miss, and the SE-bytes field specifies the number of bytes that were sent from the SE.)

The SE's transaction logging format for Windows Media Streaming is consistent with that of the Windows Media Services and the World Wide Web Consortium (W3C)-compliant log format. A log line is written for every stream accessed by the client. The location of the log is not configurable. These logs can be exported using FTP. When transaction logging is enabled, daemons create a separate *working.log* file in /local1/logs/export for WMT transactions.

All client information in the transaction logs is sent to the origin server by default.



### Note

Transaction logs are generated by the client or the downstream SE and sent to the upstream SE, unless there is a disconnect before the log is sent.



### Note

All WMT playable contents can be delivered by either HTTP or RTSP, based on the request. Any content that is cached by the WMT is stored using the RTSP scheme, regardless of whether the content was cached due to an HTTP or RTSP request. Therefore, in the **show** command, the content displays as RTSP.

See the following sections for more information:

- [Log Formats Accepted by Windows Media Services 9, page 10-47](#)
- [Windows Media Streaming Transaction Log Fields, page 10-48](#)

## Log Formats Accepted by Windows Media Services 9

Windows Media Players connect to a Windows Media server using the following protocols:

- Windows Media Players earlier than Version 9.0 use HTTP/1.0 or the MMS protocol.
- Windows Media Player Version 9.0 uses HTTP/1.1 and RTSP.

Depending on the version of the Windows Media Player, logs are sent in different formats, such as text, binary, or Extensible Markup Language (XML). [Table 10-31](#) describes the log formats accepted by Windows Media Services Version 9.0.

**Table 10-31 Windows Media Services Version 9.0 Log Formats**

| Protocol | Player and Distributor                                                                                                                                                                                                    | Log Type                                                          |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| HTTP/1.0 | Windows Media Player earlier than Version 9.0<br>SE (caching and proxy server) is running Windows Media Services Version 9.0 and streaming from a Windows Media server that is running Windows Media Services Version 4.1 | World Wide Web Consortium (W3C) standard space-delimited text log |
| MMS      | Windows Media Player earlier than Version 9.0                                                                                                                                                                             | Binary structure log                                              |
| HTTP/1.1 | Windows Media Player Version 9.0<br>Distribution server is running Windows Media Services Version 9.0<br>SE (caching and proxy server) is running Windows Media Services Version 9.0                                      | XML structure log                                                 |
| RTSP     | Windows Media Player Version 9.0<br>Distribution server is running Windows Media Services Version 9.0<br>SE (caching and proxy server) is running Windows Media Services Version 9.0                                      | XML structure log                                                 |



**Note**

Extensible Markup Language (XML) logging for MMS-over-HTTP and MMS-over-RTSP (RTSP over Windows Media Services Version 9.0) is supported. The posted XML log file from the Windows Media Player to the SE (Windows Media server) can be parsed and saved to the normal Windows Media transaction logs that are stored on the SE.

## Windows Media Streaming Transaction Log Fields



**Note**

When a client closes a connection, a Logplaystats message is sent. When Fast Cache is enabled, the client communicates by sending a sendevent. which means there is a sendevent every time the client pauses and plays the content. When Fast Cache is enabled and a client closes the connection there are two transaction log entries, sendevent and Logplaystats.



**Note**

Changing the time zone on an SE does not affect the log entry timestamps, only the log filename. The log entries always use UTC.

[Table 10-32](#) describes the fields for the Windows Media Streaming transaction log.

**Table 10-32**      **Windows Media Streaming Transaction Log Fields**

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Sample Value                         | Client Data Reported |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|----------------------|
| c-ip        | The source Internet Protocol (IP) address of the connected socket. This may be the IP address of a proxy server or firewall.                                                                                                                                                                                                                                                                                                                                                              | 157.56.219.146                       | Unicast<br>Multicast |
| date        | Date, in international date format, when a client is connected.                                                                                                                                                                                                                                                                                                                                                                                                                           | 2001-04-19                           | Unicast<br>Multicast |
| time        | Time when the client is connected. The time format is either in Coordinated Universal Time (UTC) or local time, depending on how the logging plug-in is configured.                                                                                                                                                                                                                                                                                                                       | 15:30:30                             | Unicast<br>Multicast |
| c-dns       | This field is always blank.                                                                                                                                                                                                                                                                                                                                                                                                                                                               | —                                    | Unicast<br>Multicast |
| cs-uri-stem | The path (requested URL without the protocol type, host, port number, and question mark) to the content that was requested. See the <b>cs-url</b> field for the full URL. Note that this represents a change from Windows Media Services version 4.1, in which this field contained the full URL.                                                                                                                                                                                         | /test/sample.wmv<br>or<br>/broadcast | Unicast<br>Multicast |
| c-starttime | Timestamp (in seconds, no fractions) indicating the point in the stream when the client started to render content. For live broadcasts, this field is set to 0.                                                                                                                                                                                                                                                                                                                           | 39                                   | Unicast<br>Multicast |
| x-duration  | Length of time (in seconds) of the data received by the client. For player log entries, the value does not include buffered data. For distribution server log entries, the value includes all time spent receiving data, including any buffering.                                                                                                                                                                                                                                         | 31                                   | Unicast<br>Multicast |
| c-rate      | <p>The rate at which data is sent from the server to the client. The c-rate field has the following possible values:</p> <ul style="list-style-type: none"> <li>• 0.5—Half of the real-time rate</li> <li>• 1—Real-time rate</li> <li>• 2—Twice as fast as real-time rate</li> <li>• 5—Fast forward</li> <li>• -5—Fast rewind</li> </ul> <p>If you are using Fast Streaming, these values could be considerably higher or lower depending on the content and the available bandwidth.</p> | 1                                    | Unicast<br>Multicast |

**Table 10-32** Windows Media Streaming Transaction Log Fields (continued)

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Sample Value                                           | Client Data Reported |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|----------------------|
| c-status         | Codes that describe the client status. The c-status field has the following possible codes: <ul style="list-style-type: none"> <li>200—Connection was successful</li> <li>210—Client reconnected (after first disconnecting)</li> <li>400—Requested URL was invalid</li> <li>401—Client was denied access</li> <li>404—Requested content was not found</li> <li>408—Client failed to submit a log because the client disconnected</li> <li>420—Client was disconnected and attempted to reconnect but failed. If the client attempts to reconnect, a new session is started. This code reflects the client's statistics when the client was originally disconnected. For each log entry with this code, there should be a 408 code that has the same session ID.</li> <li>500—Windows Media server encountered an internal error and stopped streaming</li> </ul> | 200                                                    | Unicast<br>Multicast |
| c-playerid       | Globally unique identifier (GUID) of the client. For player log entries, if the player is configured to not send unique player identification information to content providers, the value is: {3300AD50-2C39-46c0-AE0A-xxxxxxxxxxxx}, where x is the session ID of the client. For distribution server log entries, this value is always a series of zeroes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | {c579d042-cecc-11d1-bb31-00a0c9603954}                 | Unicast<br>Multicast |
| c-playerversion  | For player log entries, this field represents the version number of the player. For distribution server log entries, this field represents the version number of the distribution server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 6.2.5.415                                              | Unicast<br>Multicast |
| c-playerlanguage | Language and country or region code of the player.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | en-US                                                  | Unicast<br>Multicast |
| cs(User-Agent)   | Browser type used if the player was embedded in a browser. If the player was not embedded, this field refers to the user agent of the client that generated the log.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Mozilla/4.0_(compatible;_MSIE_4.01;_Windows_98)        | Unicast              |
| cs(Referer)      | URL to the web page in which the player was embedded (if it was embedded). If this is unknown, the field is blank.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | http://www.example.microsoft.com                       | Unicast              |
| c-hostexe        | For player log entries, this is the host program (.exe) that was started (for example, a web page in a browser, a Microsoft Visual Basic applet, or a stand-alone player). For distribution server log entries, this is the name of the distribution server's service program (.exe) that was started.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | iexplore.exe<br>vb.exe<br>mplayer2.exe<br>WMServer.exe | Unicast<br>Multicast |
| c-hostexever     | Host program (.exe) version number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 4.70.1215                                              | Unicast<br>Multicast |
| c-os             | Client operating system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Windows_NT                                             | Unicast<br>Multicast |



**Table 10-32** Windows Media Streaming Transaction Log Fields (continued)

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                                                          | Sample Value                                 | Client Data Reported |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|----------------------|
| c-osversion  | Version number of the client operating system.                                                                                                                                                                                                                                                                                                                                                                       | 4.0.0.1381                                   | Unicast<br>Multicast |
| c-cpu        | Client CPU type.                                                                                                                                                                                                                                                                                                                                                                                                     | Pentium                                      | Unicast<br>Multicast |
| filelength   | Length of the digital media file (in seconds). This value is zero for a stream delivered from a broadcast publishing point.                                                                                                                                                                                                                                                                                          | 60                                           | Unicast              |
| filesize     | Size of the digital media file (in bytes). This value is zero for a stream delivered from a broadcast publishing point.                                                                                                                                                                                                                                                                                              | 86000                                        | Unicast              |
| avgbandwidth | Average bandwidth (in bits per second) used by the client when connected to the server. The value is calculated across the entire duration of the connection.                                                                                                                                                                                                                                                        | 24300                                        | Unicast<br>Multicast |
| protocol     | Actual protocol used to access the content (may differ from the protocol requested by the client). A value of “Cache” indicates that a client played the content from its disk-based cache. A value of “asfm” indicates that the content was delivered using multicast transmission.                                                                                                                                 | MMST                                         | Unicast<br>Multicast |
| transport    | Transport protocol used to stream the content. Multicast content is always streamed using UDP.                                                                                                                                                                                                                                                                                                                       | UDP<br>TCP                                   | Unicast<br>Multicast |
| audiocodec   | For player log entries, this is the audio codecs used to encode the audio streams the client accessed. If multiple codecs were used, the values are delimited by a semicolon. This field contains a hyphen (-) in distribution server log entries.                                                                                                                                                                   | Microsoft_Audio_Codec                        | Unicast<br>Multicast |
| videocodec   | For player log entries, this is the video codecs used to encode the video streams the client accessed. If multiple codecs were used, the values are delimited by a semicolon. This field contains a hyphen (-) in distribution server log entries.                                                                                                                                                                   | Microsoft_MPEG-4_Video_Codec_V2              | Unicast<br>Multicast |
| channelURL   | URL to the multicast information file. This field contains a hyphen (-) in a client receiving content as a unicast stream unless the unicast stream is a result of a unicast rollover from a multicast stream.                                                                                                                                                                                                       | http://www.example.microsoft.com/channel.nsc | Unicast<br>Multicast |
| sc-bytes     | Total number of bytes the server sent to the client. The value does not include any overhead that is added by the network stack. However, protocols such as MMS, RTSP, and HTTP may introduce some overhead. Therefore, the same content streamed by using different protocols may result in different values.<br><br>This field contains a hyphen (-) in propagated cache or proxy logs and in multicast log files. | 30000                                        | Unicast              |
| c-bytes      | Number of bytes received by the client from the server. The value does not include any overhead that is added by the network stack. However, protocols such as MMS, RTSP, and HTTP may introduce some overhead. Therefore, the same content streamed by using different protocols may result in different values. If the c-bytes and sc-bytes fields are not identical, packet loss occurred.                        | 28583                                        | Unicast<br>Multicast |

**Table 10-32** Windows Media Streaming Transaction Log Fields (continued)

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                              | Sample Value | Client Data Reported |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------------------|
| s-pkts-sent             | Number of content packets sent by the server to a connected client. The value does not include TCP or UDP packets. This field contains a hyphen (-) in propagated cache or proxy logs and in multicast log files.                                                                                                                                                                                                        | 55           | Unicast              |
| c-pkts-received         | Number of packets from the server (s-pkts-sent) that are received correctly by the client on the first try. Packets that are not received correctly on the first try can be recovered if they are resent through UDP. Packets that are not recovered through UDP resend are considered lost in the network. You can recover these packets if error correction is enabled. The value does not include TCP or UDP packets. | 50           | Unicast<br>Multicast |
| c-pkts-lost-client      | Packets lost that were not recovered at the client layer through error correction or at the network layer through UDP resends during transmission from server to client. These packets are sent by the Windows Media server but never played by the client. The value does not include TCP or UDP packets.                                                                                                               | 5            | Unicast<br>Multicast |
| c-pkts-lost-net         | Number of packets lost on the network layer. You can still recover these packets if error correction is enabled. The value does not include TCP or UDP packets.                                                                                                                                                                                                                                                          | 2            | Unicast<br>Multicast |
| c-pkts-lost-cont-net    | Maximum number of continuously lost packets on the network layer during transmission from server to client. If the value is high, the network conditions were bad with long periods of time during which the client received no packets. The value does not include TCP or UDP packets.                                                                                                                                  | 2            | Unicast<br>Multicast |
| c-resendreqs            | Number of client requests to receive new packets. This field contains a zero unless the client is using UDP resend.                                                                                                                                                                                                                                                                                                      | 5            | Unicast<br>Multicast |
| c-pkts-recovered-ECC    | Packets lost in the network (c-pkts-lost-net) that were repaired and recovered at the client layer because error correction was enabled. Error correction is the only means of packet recovery for multicast streams. Packets repaired and recovered at the client layer are equal to the difference between the c-pkts-lost-net and c-pkts-lost-client fields. The value does not include TCP or UDP packets.           | 3            | Unicast<br>Multicast |
| c-pkts-recovered-resent | Number of packets recovered because they were resent through UDP. The value does not include TCP or UDP packets. This field contains a zero unless the client is using UDP resend.                                                                                                                                                                                                                                       | 5            | Unicast<br>Multicast |
| c-buffercount           | Number of times the client buffered while playing the stream.                                                                                                                                                                                                                                                                                                                                                            | 4            | Unicast<br>Multicast |
| c-totalbuffertime       | Time (in seconds) the client used to buffer the stream. If the client buffers more than once before a log entry is generated, c-totalbuffertime is the total amount of time the client spent buffering.                                                                                                                                                                                                                  | 6            | Unicast<br>Multicast |
| c-quality               | The lowest amount of stream quality reported by the player during the playback of the stream.                                                                                                                                                                                                                                                                                                                            | 96           | Unicast<br>Multicast |

**Table 10-32** Windows Media Streaming Transaction Log Fields (continued)

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                         | Sample Value                                                                                                                                                                                         | Client Data Reported |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| s-ip           | IP address of the server that received the log file. For multicast log files, this value is the IP address of the web server on which Wmsiislog.dll is installed.                                                                                                                                                                                                                   | 224.24.41.189                                                                                                                                                                                        | Unicast<br>Multicast |
| s-dns          | Domain Name System (DNS) name of the server that received the log file. This field contains a hyphen (-) in multicast log files.                                                                                                                                                                                                                                                    | media.server.com<br>pany.com                                                                                                                                                                         | Unicast              |
| s-totalclients | Number of clients connected to the server (but not necessarily streaming) at the time the event was logged. This field contains a hyphen (-) in propagated cache or proxy logs and in multicast log files.                                                                                                                                                                          | 20                                                                                                                                                                                                   | Unicast              |
| s-cpu-util     | Average load on the server processor (0 to 100 percent). If multiple processors exist, this value is the average for all processors. This field contains a hyphen (-) in propagated cache or proxy logs and in multicast log files.                                                                                                                                                 | 40                                                                                                                                                                                                   | Unicast              |
| cs-username    | The user name the client provided during authentication. This field contains a value only if authorization and authentication plug-ins are enabled. If an anonymous authentication method is used, this field contains a hyphen (-).                                                                                                                                                | JSmith                                                                                                                                                                                               | Unicast              |
| s-sessionid    | A session identifier the server uses to track a stream session. This is important for tracking multiple log entries to the same session. Note that if Windows Media Player version 6.4 received content over HTTP, the s-sessionid value changes for each log entry, even if the entries are for the same session.                                                                  | 123456                                                                                                                                                                                               | Unicast              |
| s-contentpath  | The actual content that streamed. A plug-in may resolve a requested path to another path. If the client was redirected, this field represents the location to which the client was redirected.                                                                                                                                                                                      | file://C:\WMPub\<br>WMRoot\Encoder<br>_ad.wmv<br><br>or<br><br>http://www.examp<br>le.microsoft.com/<br>speech.wma                                                                                   | Unicast              |
| cs-url         | The actual URL requested by the client.<br><br>For multicast clients, this value is the multicast IP address and port. However, Windows Media Player 9 Series and the Windows Media Player 9 Series ActiveX control multicast clients submit the multicast IP address and port, followed by the IP address of the network interface from which the server broadcasts the multicast. | mms://microsoft.co<br>m/mycontent.wmv<br><br>asfm://206.73.118.2<br>54:26502<br><br>For Windows<br>Media Player 9<br>Series clients:<br><br>asfm://multicast IP<br>address:port/Server<br>IP address | Unicast<br>Multicast |

**Table 10-32** Windows Media Streaming Transaction Log Fields (continued)

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Sample Value   | Client Data Reported |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------------|
| cs-media-name   | If the client was receiving content from a playlist, this is the media element the client was receiving. The value is derived from the mediaName attribute of the playlist media element. If the mediaName attribute is not present, the value in this field is derived from the file name value. This field is blank if the client was not receiving content from a playlist.<br><br>Alternatively, this entry can be specified in the announcement file to classify logs according to user or content.                                                                                                                                               | /ads/MyAd2.asf | Unicast              |
| c-max-bandwidth | The maximum bandwidth rate (in bits per second) of the client. This value can be used to determine whether clients have the capacity for higher bandwidth content. The value recorded for this field can have the following types of values: <ul style="list-style-type: none"> <li>Valid number of bps reported from the client, such as 38400.</li> <li>Undetermined amount, logged as 0.</li> <li>Very large amount that cannot be accurately measured but is greater than 1000000 and less than 1000000000 bps, logged as a hyphen (-).</li> <li>Hyphen (-), when a file is being played from the local cache and no bandwidth is used.</li> </ul> | 384000         | Unicast<br>Multicast |
| cs-media-role   | A user-defined value that identifies the role of a media element in a playlist. Typically, this field is used to enable advertisement logging. If the media element does not have a role attribute, or if the client was not receiving content from a playlist, this field is blank. Alternatively, this entry can be specified in the announcement file to classify logs according to user or content.                                                                                                                                                                                                                                                | Ad             | Unicast              |
| s-proxied       | Indicates whether the client connected through a cache or proxy server. A value of 0 indicates no cache or proxy server was involved. A value of 1 indicates a cache or proxy server was involved.                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 1              | Unicast              |

## Movie Streamer Transaction Log Fields



### Note

Changing the time zone on an SE does not affect the log entry timestamps, only the log filename. The log entries always use UTC.

[Table 10-33](#) describes the fields for the Movie Streamer transaction log.

**Table 10-33** Movie Streamer Transaction Log Fields

| Field | Description                      |
|-------|----------------------------------|
| c-ip  | Client IP address.               |
| date  | Current log entry creation date. |

**Table 10-33** *Movie Streamer Transaction Log Fields (continued)*

| Field              | Description                                                           |
|--------------------|-----------------------------------------------------------------------|
| time               | Current log entry creation time.                                      |
| c-dns              | Resolved DNS of the client.                                           |
| cs-uri-stem        | Client-requested URL.                                                 |
| c-starttime        | The play start time related to session start time in seconds.         |
| x-duration         | Current session duration in seconds.                                  |
| c-rate             | Play rate (trick mode). Currently, this field has a fixed value of 1. |
| c-status           | RTSP status code.                                                     |
| c-playerid         | Client IP address (used for identification).                          |
| c-playerversion    | The version of the client media player.                               |
| c-playerlanguage   | The language of client media player.                                  |
| cs(User-Agent)     | The user-agent description of the client media player.                |
| c-os               | The operating system description of the client media player.          |
| c-osversion        | The operating system version of the client media player.              |
| c-cpu              | This field contains a hyphen (-) at all times.                        |
| filelength         | Content duration in seconds.                                          |
| filesize           | Content file size in bytes.                                           |
| avgbandwidth       | Content bitrate in bits per second (bps).                             |
| protocol           | Media data transport protocol (RTP or RTSP).                          |
| transport          | Media data transport type (UDP or TCP).                               |
| audiocodec         | Audio codec information.                                              |
| videocodec         | Video codec information.                                              |
| sc-bytes           | Bytes sent from the server to the client.                             |
| cs-bytes           | Bytes sent from the client to the server.                             |
| c-bytes            | Bytes received by the client.                                         |
| s-pkts-sent        | Packets sent by the server.                                           |
| c-pkts-received    | Packets received by the client.                                       |
| c-pkts-lost-client | Client packets lost.                                                  |
| c-buffercount      | Client buffer count. Currently, this field has a fixed value of 1.    |
| c-totalbuffertime  | Client buffer delay time in seconds.                                  |
| c-quality          | Client QoS level in current session.                                  |
| s-ip               | Server IP address.                                                    |
| s-dns              | Server DNS.                                                           |
| s-totalclients     | Current number of clients connecting to server.                       |
| s-cpu-util         | Current CPU usage. Currently, this field has a fixed value of 0.      |
| cs-uri-query       | The query URI sent from the client.                                   |

**Table 10-33** *Movie Streamer Transaction Log Fields (continued)*

| Field      | Description                       |
|------------|-----------------------------------|
| c-username | The username sent from the client |
| sc(Realm)  | The server's realm.               |

## Flash Media Streaming Transaction Log Fields

The Flash Media Streaming transaction logs consist of the access log and the authorization log.

[Table 10-34](#) describes the fields for the Flash Media Streaming access log and authorization log. All fields listed in [Table 10-34](#) are logged for the access log, but only a selection are logged for the authorization log.


**Note**

When the data for a field contains a space or delimiter, the data is enclosed in double quotation marks. The double quotation marks surrounding the data are not part of the data, but are present for better parsing of the data. This applies to the tz, x-ctx, x-adaptor, x-vhost, s-uri, c-referrer, c-user-agent, cs-bytes, sc-bytes, and x-sname fields.

The following formats apply to the fields in [Table 10-34](#):

Date—YYYY-MM-DD

Time—hh:mm:ss

Time zone—Contains a string such as “UTC,” “Pacific Daylight Time,” or “Pacific Standard Time”


**Note**

Changing the time zone on an SE does not affect the log entry timestamps, only the log filename. The log entries always use UTC.

**Table 10-34** *Flash Media Streaming Access and Authorization Log Fields*

| Field      | Description                                                                         | Authorization Log Field? |
|------------|-------------------------------------------------------------------------------------|--------------------------|
| x-event    | Type of event. See <a href="#">Table 10-36</a> for a list of the event types.       | Yes                      |
| x-category | Event category. See <a href="#">Table 10-36</a> for a list of the event categories. | Yes                      |
| date       | Date of the event.                                                                  | Yes                      |
| time       | Time the event occurred.                                                            | Yes                      |
| tz         | Time zone information.                                                              | No                       |
| x-ctx      | Event-dependent context information.                                                | No                       |
| s-ip       | IP address or addresses of the server.                                              | No                       |
| x-pid      | Server process ID.                                                                  | Yes                      |
| x-cpu-load | CPU load.                                                                           | No                       |
| x-mem-load | Memory usage (as reported by the <code>getServerStats()</code> method).             | No                       |
| x-adaptor  | Adaptor name.                                                                       | Yes                      |
| x-vhost    | Virtual host name.                                                                  | No                       |

**Table 10-34**      **Flash Media Streaming Access and Authorization Log Fields (continued)**

| Field      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Authorization Log Field? |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| x-app      | Application names.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Yes                      |
| x-appinst  | Application instance names.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Yes                      |
| x-duration | Duration of a stream or session event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | No                       |
| x-status   | <p>The status code. The status code for the authorization log is a ten-character string that represents the severity, category, and message ID. For information on the status codes for the access log, see the <a href="#">“Status Codes in Flash Media Streaming Access Logs”</a> section on page 10-60.</p> <p>The first three characters represent severity and have the following values:</p> <ul style="list-style-type: none"> <li>• (w)—Warning</li> <li>• (e)—Error</li> <li>• (i)—Information</li> <li>• (d)—Debug</li> <li>• (s)—Trace from server-side script</li> <li>• (—)—Unknown</li> </ul> <p>The next three characters represent the category and have the following values:</p> <ul style="list-style-type: none"> <li>• 257—TCSservice</li> <li>• 258—TCServer</li> <li>• 259—Presence</li> <li>• 260—Storage</li> <li>• 261—Stream</li> <li>• 262—SMTP</li> <li>• 263—Adaptor</li> <li>• 264—JavaScript</li> <li>• 265—TCApplication</li> <li>• 266—TCCconnector</li> <li>• 267—Admin</li> <li>• 268—SharedObject</li> <li>• 269—Configuration</li> <li>• 270—VirtualHost</li> <li>• 271—SSL</li> </ul> <p>The last four characters represent the message ID. The message ID records information about operation of the Flash Media Server. For more information, see the <i>Adobe Flash Media Server 3.5 Configuration and Administration Guide</i>.</p> | Yes                      |
| c-ip       | Client IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Yes                      |
| c-protocol | Connection protocol (RTMP).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | No                       |
| s-uri      | URI of the Flash Media Server application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | No                       |

**Table 10-34** *Flash Media Streaming Access and Authorization Log Fields (continued)*

| Field           | Description                                                                                                                                                                                                                                                                                                                                                         | Authorization Log Field? |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| cs-uri-stem     | The stem portion of the s-uri field.                                                                                                                                                                                                                                                                                                                                | No                       |
| cs-uri-query    | The query portion of the s-uri field.                                                                                                                                                                                                                                                                                                                               | No                       |
| c-referrer      | URI of the referrer.                                                                                                                                                                                                                                                                                                                                                | No                       |
| c-user-agent    | User agent.                                                                                                                                                                                                                                                                                                                                                         | No                       |
| c-client-id     | Client ID.                                                                                                                                                                                                                                                                                                                                                          | No                       |
| cs-bytes        | This field shows the number of bytes transferred from the client to the server.<br><br>This information can be used to bill customers per session. To calculate the bandwidth usage per session, subtract the cs-bytes value in the “connect” event from the cs-bytes value in the “disconnect” event.                                                              | No                       |
| sc-bytes        | This field shows the number of bytes transferred from the server to the client.<br><br>This information can be used to bill customers per session. To calculate the bandwidth usage per session, subtract the sc-bytes value in the “connect” event from the sc-bytes value in the “disconnect” event                                                               | No                       |
| c-connect-type  | Type of connection received by the server: <ul style="list-style-type: none"> <li>• Normal—Connection from a client, such as Flash Player</li> <li>• Group—Connection between an edge server and an origin server</li> <li>• Virtual—Client connection that goes through an edge server, using the group connection between the servers for transmission</li> </ul> | No                       |
| x-sname         | Stream name.                                                                                                                                                                                                                                                                                                                                                        | Yes                      |
| x-sname-query   | Query portion of the stream URI specified in play or publish.                                                                                                                                                                                                                                                                                                       | No                       |
| x-suri-query    | Same as x-sname-query.                                                                                                                                                                                                                                                                                                                                              | No                       |
| x-suri-stem     | This is a composite field made up of cs-uri-stem + x-sname + x-file-ext.                                                                                                                                                                                                                                                                                            | No                       |
| x-suri          | This is a composite field made up of cs-uri-stem + x-sname + x-file-ext + x-sname-query.                                                                                                                                                                                                                                                                            | No                       |
| x-file-name     | Full path of the file representing the x-sname stream.                                                                                                                                                                                                                                                                                                              | Yes                      |
| x-file-ext      | Stream type (FLV or MP3).                                                                                                                                                                                                                                                                                                                                           | Yes                      |
| x-file-size     | Stream size in bytes.                                                                                                                                                                                                                                                                                                                                               | Yes                      |
| x-file-length   | Stream length in seconds.                                                                                                                                                                                                                                                                                                                                           | Yes                      |
| x-spos          | Stream position.                                                                                                                                                                                                                                                                                                                                                    | Yes                      |
| cs-stream-bytes | This field shows the number of bytes transferred from the client to the server per stream.<br><br>To calculate the bandwidth usage per stream, subtract the cs-stream-bytes value in the “publish” event from the cs-stream-bytes value in the “unpublish” event.                                                                                                   | Yes                      |



**Table 10-34** *Flash Media Streaming Access and Authorization Log Fields (continued)*

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Authorization Log Field? |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| sc-stream-bytes     | <p>This field shows the number of bytes transferred from the server to the client per stream. To calculate the bandwidth usage per stream, subtract the sc-stream-bytes value in the “play” event from the sc-stream-bytes value in the “stop” event.</p> <p>The value of sc-stream-bytes can be greater than x-file-size when streaming files that are not encoded in FLV format, such as MP3 files.</p> <p><b>Note</b> The value of sc-stream-bytes is not necessarily the same as the value of the QoS ByteCount property.</p> | Yes                      |
| x-service-name      | Name of the service providing the connection (only applicable to certain connection types).                                                                                                                                                                                                                                                                                                                                                                                                                                       | No                       |
| x-sc-qos-bytes      | Number of bytes sent to the client for quality of service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | No                       |
| x-comment           | Comments.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | No                       |
| x-sid               | The ID of a stream. This ID is unique for the client session but not across sessions.                                                                                                                                                                                                                                                                                                                                                                                                                                             | No                       |
| x-trans-sname       | The name of the stream that the server transitions from (the original stream).                                                                                                                                                                                                                                                                                                                                                                                                                                                    | No                       |
| x-trans-sname-query | The query stream portion of the stream name for the stream that the server transitions from.                                                                                                                                                                                                                                                                                                                                                                                                                                      | No                       |
| x-trans-file-ext    | The file extension portion of the stream name for the stream that the server transitions from.                                                                                                                                                                                                                                                                                                                                                                                                                                    | No                       |
| x-plugin            | Name of the plug-in. This field is only available in authorization (auth-) events.                                                                                                                                                                                                                                                                                                                                                                                                                                                | No                       |
| x-page-url          | The URL of the web page in which the client SWF file is embedded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | No                       |
| x-smax-rec-size     | The maximum file size of a recorded stream.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | No                       |
| x-smax-rec-duration | The maximum duration of a recorded stream.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | No                       |
| x-trans-mode        | The transition mode sent by the client in the NetStream.play2() call.                                                                                                                                                                                                                                                                                                                                                                                                                                                             | No                       |
| x-offset            | When a stream is reconnected, the offset value indicates where to resume streaming.                                                                                                                                                                                                                                                                                                                                                                                                                                               | No                       |
| c-spos              | The client stream position when a “client-pause” or “client-seek” event is logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                | No                       |
| x-eid               | An event ID received by Authorization plug-in. This event is visible only in the auth.log file. This field is empty in the access.log file.                                                                                                                                                                                                                                                                                                                                                                                       | No                       |
| x-codec-type        | Codec type of the frame retrieved in the Authorization plug-in’s E_CODEC event. This event is visible only in the auth.log file. This field is empty in the access.log file.                                                                                                                                                                                                                                                                                                                                                      | No                       |
| x-codec             | Codec value of the “x-codec-type” retrieved in the Authorization plug-in’s E_CODEC_CHANGE event. This event is visible only in the auth.log file. This field is empty in the access.log file.                                                                                                                                                                                                                                                                                                                                     | No                       |

## Status Codes in Flash Media Streaming Access Logs

The event status codes are based on HTTP response codes. [Table 10-35](#) describes the status codes for the Flash Media Streaming access log.

**Table 10-35** Flash Media Streaming Event Status Codes

| Field                                                        | Symbol                    | Status Code | Description                                                                                                                           |
|--------------------------------------------------------------|---------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------|
| connect pending                                              | status_continue           | 100         | Waiting for the application to authenticate.                                                                                          |
| disconnect                                                   | status_admin_command      | 102         | Client disconnected due to admin command.                                                                                             |
| disconnect                                                   | status_shutdown           | 103         | Client disconnected due to server shutdown (or application unloaded).                                                                 |
| connect, publish, unpublish, play, record, record stop, stop | status_OK                 | 200         | Successful.                                                                                                                           |
| play, stop                                                   | status_transition         | 210         | A transition between streams has occurred.                                                                                            |
| connect                                                      | status_unavailable        | 302         | Application currently unavailable.                                                                                                    |
| connect, publish, play                                       | status_bad_request        | 400         | Bad request; invalid parameter or client connected to server using an unknown protocol.                                               |
| connect, play, publish                                       | status_unauthorized       | 401         | Connection rejected by application script or access denied by application.                                                            |
| connect                                                      | status_forbidden          | 403         | Connection rejected by Authorization plug-in or connection rejected due to invalid URI.                                               |
| connect, play                                                | object_not_found          | 404         | Application or stream not found.                                                                                                      |
| play                                                         | client_disconnect         | 408         | Stream stopped because client disconnected.                                                                                           |
| connect, publish                                             | status_conflict           | 409         | Resource limit exceeded or stream is already being published. Can also mean that a change has been made by the Authorization plug-in. |
| connect                                                      | status_lic_limit_exceeded | 413         | License limit exceeded.                                                                                                               |
| play, publish                                                | unsupported_type          | 415         | Unsupported media type.                                                                                                               |
| disconnect                                                   | data_exceeded             | 416         | Message queue too large; disconnect the client.                                                                                       |
| connect                                                      | chunkstream_error         | 417         | Unable to process unknown data type.                                                                                                  |
| disconnect                                                   | cannot_broadcast          | 418         | Client does not have privilege to broadcast.                                                                                          |
| disconnect                                                   | cannot_screenshare        | 419         | License to receive screen sharing video failed.                                                                                       |
| disconnect                                                   | remote_link_closed        | 420         | Close downstream connection.                                                                                                          |

**Table 10-35** *Flash Media Streaming Event Status Codes (continued)*

| Field            | Symbol                      | Status Code | Description                                                                                         |
|------------------|-----------------------------|-------------|-----------------------------------------------------------------------------------------------------|
| connect          | process_msg_failed          | 422         | Unable to process message received when client connection was in pending or closed state.           |
| disconnect       | process_msg_exception       | 423         | Error handling message.                                                                             |
| disconnect       | process_remote_msg_failed   | 424         | Expected response not provided when command was issued.                                             |
| disconnect       | process_admin_msg_failed    | 425         | Expected response not provided when issued an admin command.                                        |
| disconnect       | process_rtmp_S2S_msg_failed | 426         | Expected response not provided when command was issued.                                             |
| disconnect       | write_error                 | 427         | Client is not connected or client terminated; unable to write data.                                 |
| disconnect       | invalid_session             | 428         | Client connection invalid; closed due to inactive or idle status.                                   |
| disconnect       | gc_client                   | 429         | Unable to obtain ping response or client states not connected.                                      |
| disconnect       | remote_onstop               | 430         | Upstream connection closed.                                                                         |
| disconnect       | remote_on_client_disconnect | 431         | Upstream connection closed because the last client disconnected.                                    |
| disconnect       | gc_idle_client              | 432         | Flash Media Server autoclose feature automatically closed the connection.                           |
| disconnect       | swf_hash_fail               | 433         | SWF verification failure.                                                                           |
| disconnect       | swf_hash_timeout            | 434         | SWF verification timeout.                                                                           |
| disconnect       | encoding_mismatch_error     | 435         | Client disconnected due to incompatibility with object encoding.                                    |
| disconnect, play | server_internal_error       | 500         | Server internal error.                                                                              |
| connect          | bad_gateway                 | 502         | Bad gateway.                                                                                        |
| connect          | service_unavailable         | 503         | Service unavailable; for instance, too many connections pending for authorization by access module. |
| disconnect       | js_disconnect               | 600         | Application disconnect.                                                                             |
| disconnect       | js_close_previous_client    | 601         | Network connection was closed or reused.                                                            |
| disconnect       | js_exception                | 602         | An unknown exception is thrown from the JS engine.                                                  |
| disconnect       | js_chunkstream_error        | 603         | Bad application data.                                                                               |
| disconnect       | js_debug_forbidden          | 604         | Application does not allow debug connections.                                                       |
| play             | js_gc_object                | 605         | ~fcteststreamjshook() clean up.                                                                     |

## Events in Flash Media Streaming Access Logs

Table 10-36 describes the event types in the Flash Media Streaming access log and the associated category for each event.

**Table 10-36 Flash Media Streaming Access Logs—Events**

| Event            | Category | Description                                                                                                                                                                                   |
|------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| connect-pending  | session  | Client connects to the server, waiting for the client to be authenticated.                                                                                                                    |
| connect          | session  | Client connects to the server.                                                                                                                                                                |
| connect-continue | session  | A checkpoint event that provides updates of a corresponding connect event at intervals. Use the c-client-id field to find the corresponding connect event.                                    |
| disconnect       | session  | Client disconnects.                                                                                                                                                                           |
| publish          | stream   | Client publishes a live stream.                                                                                                                                                               |
| unpublish        | stream   | Client unpublishes a live stream.                                                                                                                                                             |
| publish-continue | stream   | A checkpoint event that provides updates of a corresponding publish event at intervals. Use the x-sid field (stream id) and the c-client-id field to find the corresponding publish event.    |
| play             | stream   | Client plays a stream.                                                                                                                                                                        |
| play-continue    | stream   | A checkpoint event that provides updates of a corresponding play event at intervals. Use the x-sid field (stream id) with the c-client-id field to find the corresponding play event.         |
| pause            | stream   | Client pauses stream.                                                                                                                                                                         |
| unpause          | stream   | Client resumes playing stream.                                                                                                                                                                |
| client-pause     | stream   | Client smart pauses a stream. The stream is paused but the server still sends data to the client so the player has enough data to play when the client unpauses.                              |
| client-unpause   | stream   | Client smart unpauses a stream.                                                                                                                                                               |
| seek             | stream   | Client seeks in a stream.                                                                                                                                                                     |
| stop             | stream   | Client stops playing or publishing a stream.                                                                                                                                                  |
| record           | stream   | Client begins recording a stream.                                                                                                                                                             |
| recordstop       | stream   | Client stops recording a stream.                                                                                                                                                              |
| start-transmit   | stream   | The server received a “startTransmit” command. This command asks the server to transmit more data because the buffer is running low.                                                          |
| stop-transmit    | stream   | The server received a “stopTransmit” command. This command asks the server to suspend transmission until the client sends a “startTransmit” event because there is enough data in the buffer. |
| server-start     | server   | Server has started.                                                                                                                                                                           |
| server-stop      | server   | Server has stopped.                                                                                                                                                                           |
| vhost-start      | vhost    | A virtual host has started.                                                                                                                                                                   |
| vhost-stop       | vhost    | A virtual host has stopped.                                                                                                                                                                   |

**Table 10-36** *Flash Media Streaming Access Logs—Events (continued)*

| Event             | Category      | Description                                                                                                                                                                      |
|-------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| app-start         | application   | An application instance has started.                                                                                                                                             |
| app-stop          | application   | An application instance has stopped.                                                                                                                                             |
| auth-connect      | authorization | Client connects to server. This event occurs if an Authorization plug-in is present to handle the event.                                                                         |
| auth-play         | authorization | Client plays a stream. This event occurs if an Authorization plug-in is present to handle the event.                                                                             |
| auth-publish      | authorization | Client publishes a live stream. This event occurs if an Authorization plug-in is present to handle the event.                                                                    |
| auth-seek         | authorization | Client jumps to a new location within a recorded stream. This event occurs if an Authorization plug-in is present to handle the event.                                           |
| filenametransform | authorization | A virtual stream path has been mapped to a physical location. This event occurs if an Authorization plug-in is present to handle the event.                                      |
| auth-record       | authorization | Client begins recording a stream. This event occurs if an Authorization plug-in is present to handle the event.                                                                  |
| codechange        | authorization | The publisher codec changes during a live event. Logs data to the x-codec-type and x-codec fields. This event occurs if an Authorization plug-in is present to handle the event. |

## Service Router Transaction Log Fields



### Note

Changing the time zone on an SE does not affect the log entry timestamps, only the log filename. The log entries always use UTC.

Table 10-37 describes the fields for the Service Router transaction log.

**Table 10-37** *Service Router Transaction Log Fields*

| Field      | Description                                                                                                                                                          |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| c-ip       | The source Internet Protocol (IP) address of the connected socket. This may be the IP address of a proxy server or firewall.                                         |
| user-agent | Browser type used if the player was embedded in a browser. If the player was not embedded, this field refers to the user agent of the client that generated the log. |
| date       | Date, in international date format, when a client is connected.                                                                                                      |
| time       | Time when the client is connected. The time format is either in Coordinated Universal Time (UTC) or local time, depending on how the logging plug-in is configured.  |
| url        | The URL requested by the client.                                                                                                                                     |

**Table 10-37**     **Service Router Transaction Log Fields (continued)**

| Field         | Description                                        |
|---------------|----------------------------------------------------|
| protocol      | The protocol used to access the content.           |
| server-picked | The Service Engine selected by the Service Router. |
| status        | The status code.                                   |

**Note**

For cross-domain requests, the crossdomain.xml or clientaccesspolicy.xml file served by the SR is logged as 200 OK, and the request redirect is logged as a 302. For more information about cross-domain, see the [“Cross-Domain Policy” section on page 1-27](#).

## Where to Go Next

For the most current ECDS hardware and software support information, see the [Cisco ECDS 2.5 Release Notes](#) and the Cisco ECDS 2.5 Software Administration Configuration Guide.



# CHAPTER 11

## Maintaining the Enterprise CDS

---

The following sections describe how to maintain the ECDS:

- [Upgrading Software, page 11-1](#)
- [Finding the Device Software Version, page 11-9](#)
- [Rebooting Devices, page 11-9](#)
- [Deleting a Device, page 11-10](#)
- [Replacing a Device, page 11-13](#)
- [Backup and Recovery, page 11-16](#)
- [Disk Maintenance, page 11-19](#)



**Tip**

For information about database maintenance, see the [“Scheduling Database Maintenance”](#) section on page 5-75 of Chapter 5, “Configuring the Service Engine.”

---

## Upgrading Software

To upgrade the software images on your Cisco ECDS appliances:

1. [Obtaining the Upgrade, page 11-1](#)
2. [Pre-positioning the Upgrade Software File \(optional\), page 11-2](#)
3. [Configuring the Software Image Settings, page 11-2](#)
4. [Upgrading the Software, page 11-5](#)

## Obtaining the Upgrade

Refer to the [Release Notes for Cisco ECDS 2.5](#) on Cisco.com for information about obtaining the software upgrade. Put the upgrade file on an FTP or HTTP server.

## Pre-positioning the Upgrade Software File (optional)

A software file is pre-positioned in the same manner as any other content item. Pre-positioning allows you to conserve bandwidth usage across the WAN and avoid congesting your network during updates. The software file is fetched one time from the origin server, replicated across your network, and stored in Service Engine caches in your LAN.

To pre-position a software file, you must complete the following tasks:

- Define a delivery service.
- Assign devices to the delivery service.
- Define the software file that you want to pre-position by using a Manifest file or the CDSM delivery service content page.
- Check the device replication status.

See [Chapter 8, “Configuring Services”](#) for more information.

**Note**

Only Service Engines that are assigned to the delivery service can be updated using pre-positioned software files. Service Routers and CDSMs do not have pre-positioned content; therefore, you cannot use the pre-positioned method for device updates for these devices.

### Sample Manifest File to Pre-position a Software File

You can use the following sample Manifest file to pre-position a software file by replacing the URL with a valid software file URL:

```
<CdnManifest>
<item src="http://your-web-server.com/folder/upgrade_image.bin" />
</CdnManifest>
```

The server name or IP address of the URL in the Manifest file (and in the Software File URL field in the Software File Settings page must match either the Origin Server field or the Service Router Domain Name field in the Content Origin page).

## Configuring the Software Image Settings

To upgrade your ECDS software release, first configure the software image settings:

- Step 1** Choose **System > Software Image Management**. The Software Files Table page is displayed.
- Step 2** Click the **Create New** icon in the task bar. The Software Image page is displayed ([Figure 11-1](#)).



Figure 11-1 Software Image Page

The screenshot shows the 'Software Image Management' page. At the top, there's a 'System Status' section indicating '1 Device, Critical' and '2 Services, Critical'. Navigation tabs for 'Devices', 'Services', and 'System' are visible. The main section is titled 'Creating New Software Image'. It contains a 'Software Image Settings' form with the following fields: 'Software Image URL' (with a protocol dropdown set to 'ftp'), 'Username', 'Password', 'Confirm Password', 'Software Version' (with an example '2.0.0.b.70' and a note about version formats), and 'File Size' (in bytes). A 'Validate Software Image Settings' button is below these fields. The 'Advanced Settings' section includes 'Auto Reload' (checked), 'Download Method' (radio buttons for 'Default', 'Prepositioned Only', and 'Direct Download Only'), and 'CDSM IP Address'. A 'Comments' section with a text area is at the bottom. 'Submit' and 'Cancel' buttons are in the bottom right corner.

**Step 3** In the **Software Image URL** field, enter the URL for the .bin software file that you downloaded from Cisco.com.

- a. Choose a protocol (**http** or **ftp**) from the drop-down list.
- b. Enter the URL of the software file; for example, a valid URL might look like this:

`http://internal.mysite.com/cds/ecds_2.x.x_upgd-k9.bin`

In this URL, *ecds-2.x.x-K9* is the name of the software upgrade file. (The filename might include the version number.)



**Note** If you are using a pre-positioned software file and you are entering the URL manually (rather than using the **Select File from Delivery Service** option), the server name or IP address of the URL in the Software Image URL field must match either the Origin Server field or the Service Routing Domain Name field in the Content Origin page of the delivery service. This is not a requirement if you are downloading the software file directly from the origin server. (See the “[Pre-positioning the Upgrade Software File \(optional\)](#)” section on page 11-2 for details.)

Alternatively, click **Select File from Delivery Service**. A separate window displays that allows you to choose a delivery service, set criteria, search the delivery service, and select the software file that you want to use for the software upgrade. (You must first pre-position the software file in the delivery service. See the “[Pre-positioning the Upgrade Software File \(optional\)](#)” section on page 11-2.)

- Step 4** If your server requires user login authentication, enter your username in the **Username** field and enter your login password in the **Password** field. Enter the same password in the **Confirm Password** field.
- Step 5** Enter the software version number in the **Software Version** field. You can copy this number from the version portion of the software filename in the software file URL.
- Specify the version in one of two formats: X.Y.Z-bB or X.Y.Z.b.B, where X = major version, Y = minor version, Z = maintenance version, b = build letter, and B = build number.
- Step 6** If you want the size of the software file considered during validation, enter a file size (in bytes) in the **File Size** field. If you leave this field blank, the URL is checked without regard to the software file size.
- Step 7** To validate the Software Image URL, Username, and Password fields, click the **Validate Software Image Settings** button.

When you click the **Validate Software Image Settings** button, the following occurs:

- Software file URL is resolved.
  - Connection to the software file URL is established using the username and password, if specified.
  - If a file size is specified, the actual size of the software file is obtained and compared against the value in the File Size field.
  - Message is returned, indicating success or errors encountered.
- Step 8** In the Advanced Settings section, check the **Auto Reload** check box to automatically reload a device when you upgrade the software.
- Step 9** If you want, you can choose one of three download methods:
- **Default**—Uses pre-positioned content but always falls back to direct download.
  - **Prepositioned Only**—Uses the local file copy if the software file URL references pre-positioned content and its replication status is complete.
  - **Direct Download Only**—Directly downloads the file using the software file URL.



**Note**

If you choose **Prepositioned Only**, the software file settings that you define in this page cannot be used to upgrade an ECDSM or an SR, because these devices do not have pre-positioned content.

- Step 10** For downgrades only, specify the CDSM IP address to be used for device registration in the **ECDSM IP Address** field.

The ECDSM IP Address field is the IP address of a ECDSM after the software is downgraded. (This field is optional and only applies for downgrades.) After the downgrade, the SE registers with the ECDSM with the IP address specified in this field.

- Step 11** Click **Submit**.

To delete a software file, click the **Delete** icon in the task bar.



**Caution**

If your browser is configured to save the username and password for the ECDSM, the browser auto-populates the Username and Password fields in the Software Image page. You must clear these fields before you click **Submit**.

The software file that you want to use is now registered with the ECDSM. When you perform the software upgrade or downgrade, the URL that you just registered becomes one of the choices available in the Update Software page. (See the [“Upgrading the Software”](#) section on page 11-5.)

## Upgrading the Software

When upgrading software in your ECDS network, begin with Service Engines and Service Routers before upgrading the ECDSM. The ECDSM reboots at the conclusion of the upgrade procedure, causing you to temporarily lose contact with the device and the user interface. After the ECDSM has upgraded its software and rebooted, it may be unable to communicate with devices running different versions of the ECDS software.



### Caution

Primary and standby ECDSMs must be running the same version of ECDS software. If they are not, the standby ECDSM detects this and does not process any configuration updates it receives from the primary ECDSM.

When you upgrade ECDSMs using the GUI, you need to upgrade your standby ECDSM first, and then upgrade your primary ECDSM. We also recommend that you create a database backup for the primary ECDSM and copy the database backup file to a safe place before you upgrade the software.

When you upgrade ECDSMs using the CLI, we recommend that you upgrade your primary ECDSM first, and then upgrade your standby ECDSM. Primary and standby ECDSMs must be operating with exactly the same software release as each other for failover to be successful.



### Note

For software downgrades for systems with primary and standby ECDSMs, do the following:

1. If you are using the ECDSM GUI, downgrade the standby ECDSM first, followed by the primary ECDSM.  
  
If you are using the CLI, downgrade the primary ECDSM first, followed by the standby ECDSM.
2. After downgrading the primary and standby ECDSMs, using the CLI, log in to each ECDSM and run the following commands:  

```
cms database downgrade
cms enable
```
3. Downgrade the software on the Service Routers, followed by the Service Engines.



### Caution

To upgrade the software image on a server, you first need to offload a server for maintenance. Once the server has been fully offloaded, you can upgrade the software. After updating the software, uncheck the **Server Offload** check box to allow the server to receive client requests from the Service Router. See the Server Offload field in [Table 5-1 on page 5-3 “Device Activation Fields”](#) for more information.

**Procedure**

To upgrade your software:

1. Read the [Interoperability Considerations, page 11-6](#), for information about minimizing any downtime during the upgrade process.
2. Choose one of the following upgrade procedures:
  - [Upgrading Software by Device Groups, page 11-7](#)—For upgrading multiple Service Engines. You cannot use this procedure for Service Routers or ECDSMs.
  - [Software Upgrades by Device, page 11-8](#)—For upgrading Service Routers, ECDSMs, or individual Service Engines.

## Interoperability Considerations

Typically, an ECDS network is upgraded gradually, so that your network might consist of nodes with different software versions for the duration of time it takes to upgrade all nodes. Dissimilar software versions are not supported in the long term, and only the interoperability considerations listed below are supported until all devices are running the same software version. You can expect the following behavior during an upgrade or downgrade of your network:

- ECDS network continues to operate with mixed versions up to one major or minor version difference in a deployed solution.
- New features that depend on device cooperation might not be fully functional until the ECDS network upgrade is complete, but no existing features are affected.
- While being upgraded, a node is unavailable for a short time.
- All nodes, other than the node being upgraded, continue to operate at full capacity. The availability of other nodes is not affected during an upgrade.
- Content is preserved during an upgrade or downgrade unless you remove a delivery service.
- All logs are preserved during an upgrade or downgrade, unless you change the disk configuration. Anytime disk space is reconfigured, the logs are automatically removed.

We strongly recommend that you upgrade your ECDS network devices in the following order:

1. Multicast sender Service Engines
2. Multicast receiver Service Engines
3. Non-Content Acquirer Service Engines
4. Content Acquirer Service Engines
5. Service Routers
6. Standby ECDSMs (Upgrade before primary when using the GUI only.)
7. Primary ECDSM

## Upgrading Software by Device Groups


**Note**

This procedure is for Service Engines only. Service Routers and ECDSMs cannot be associated with device groups.

To upgrade your software on multiple Service Engines:

- Step 1** Choose **Devices > Device Groups**. The Device Groups Table page is displayed.
- Step 2** Click the **Edit** icon next to the name of the device group that you want to upgrade. The Device Group page is displayed.
- Step 3** From the left-panel menu, choose **Software Update**. The Software Update for Device Group page is displayed.
- Step 4** Choose the software file URL from the Software File URL list by clicking the radio button next to the filename.
- Step 5** Click **Submit**.

To view progress on an upgrade, go to the Devices Table page (**Devices > Devices**). Software upgrade status messages are displayed in the Software Version column. These intermediate messages are also written to the system log on the Service Engines. See [Table 11-1](#) for a description of upgrade status messages.

**Table 11-1** Upgrade Status Messages

| Upgrade Status Message                  | Condition                                                                                                                                       |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Pending                                 | The request has yet to be sent from the ECDSM to the device, or receipt of the request has yet to be acknowledged by the device.                |
| Downloading                             | The download method for the software file is being determined.                                                                                  |
| Proceeding with Pre-positioned Download | The download method for the software file is detected as pre-positioned. Proceeding with download of a pre-positioned software file.            |
| Proceeding with Download                | The download method for the software file is detected as direct download. Proceeding with the request for direct download of the software file. |
| Download in Progress (Completed ...)    | Direct download of the software file is being processed. "Completed" indicates the number of megabytes processed.                               |
| Download Successful                     | The direct download of the software file has been successful.                                                                                   |
| Download Failed                         | The direct download of the software file cannot be processed. Further troubleshooting is required; see the device system message log.           |

**Table 11-1** Upgrade Status Messages (continued)

| Upgrade Status Message                  | Condition                                                                                                                     |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Proceeding with Flash Write             | A request has been made to write the software file to the device flash memory.                                                |
| Flash Write in Progress (Completed ...) | The write of the device flash memory is being processed. “Completed” indicates the number of megabytes processed.             |
| Flash Write Successful                  | The flash write of the software file has been successful.                                                                     |
| Reloading                               | A request to reload the device has been made to complete the software upgrade. The device may be offline for several minutes. |
| Reload Needed                           | A request to reload the device has not been made. The device must be reloaded manually to complete the software upgrade.      |
| Canceled                                | The software upgrade request was interrupted, or a previous software upgrade request was bypassed from the CLI.               |
| Update Failed                           | The software upgrade could not be completed. Troubleshooting is required; see the device system message log.                  |

## Software Upgrades by Device



### Note

Use this upgrade procedure for Service Routers and ECDSMs. You can also use this upgrade procedure to upgrade Service Engines one at a time.

To upgrade your software on a single device:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon of the device that you want to upgrade. The Devices home page is displayed.
- Step 3** Verify that the device is not already running the version that you plan to upgrade to, and that the current version has an upgrade path to the version that you plan to upgrade to.
- Step 4** Click **Update Software**. The Software Update page is displayed.
- Step 5** Choose the software file URL from the Software Files list by clicking the radio button next to the filename.
- Step 6** Click **Submit**, and then click **OK** to confirm your decision.

The Devices Table page is displayed again. You can monitor the progress of your upgrade from this page. Software upgrade status messages are displayed in the Software Version column. These intermediate messages are also written to the system log on the Service Engines. See [Table 11-1](#) for a description of upgrade status messages.

## Finding the Device Software Version

The ECDSM Home page gives a brief summary of the software versions in use on all the devices in the ECDS network.

To view the software version running on a particular device, choose **Devices > Devices**. The Devices Table page displays the software version for each device listed.

Clicking the **Edit** icon next to the device name in the Devices Table page displays the Devices home page, which shows the software version for that device. During an upgrade, the software version shown is not updated until the upgrade has been successfully completed.

## Rebooting Devices

You can reboot a device or device group. The ECDSM performs a controlled shutdown of all devices and then restarts the operating system on each device.

**Note**

Disconnect any external USB devices (such as drives and keyboards) before powering on the appliance. Your appliance may not boot with devices connected to the external USB ports.

- [Individual Devices, page 11-9](#)
- [Device Groups, page 11-9](#)

## Individual Devices

To reboot an individual device:

- 
- Step 1** Choose **Devices > Devices**.
  - Step 2** Click the **Edit** icon next to the device name that you want to reboot. The Devices home page is displayed.
  - Step 3** In the task bar, click the **Reload** icon. You are prompted to confirm your decision.
  - Step 4** To begin rebooting the device, click **OK**.
- 

## Device Groups

To reboot an entire device group:

- 
- Step 1** Choose **Devices > Device Groups**.
  - Step 2** Click the **Edit** icon next to the name of the device group that you want to reboot. The Device Group page is displayed.
  - Step 3** In the task bar, click the **Reboot All Devices in Device Group** icon. You are prompted to confirm your decision.

**Step 4** To begin rebooting each SE in the device group, click **OK**.

---

## Deleting a Device

You can delete a device if the device is experiencing unresolvable problems or when its network address or configuration has changed and you need to add the device back to the ECDS network using its new address and configuration information.

- [Before Deleting a Device, page 11-10](#)
- [Removing and Deregistering a Device Using CLI, page 11-11](#)
- [Removing a Device with ECDSM, page 11-12](#)
- [Deleting a Warm Standby ECDSM, page 11-13](#)

## Before Deleting a Device

Before deleting a device from your network, observe the following important notes:



### Caution

If you delete the only SR in your ECDS network, you are removing the ability of your ECDS network to fill user requests.

When you delete an SE from the ECDS network, you are removing that device and the content it contains from the routing scheme that the ECDS uses to fill user requests. Although the ECDS routes requests around SEs that are busy, offline, or missing, removing an SE may affect the speed at which the ECDS network can serve user requests.



### Note

You cannot delete an SE if it is the only device assigned to a location that is designated as the root location (Content Acquirer) for a delivery service and there are other SEs associated with the delivery service. You can delete the Content Acquirer for a delivery service if the Content Acquirer is the only SE associated with that delivery service. However, deleting the only SE in a delivery service makes the delivery service unable to deliver content. If you receive an error message referencing the Content Acquirer for a delivery service, add more SEs to that location, or change the root location by choosing an SE in a different location to be the Content Acquirer for the delivery service before attempting to delete the SE again.

Removing the device from the ECDS network involves using the CLI to shut down ECDS network services and deregister the node. If you are removing the device because of hardware failure and it cannot be accessed through its CLI, you can remove the device by using the ECDSM; however, the device continues to store its registration information until you deregister it by using the CLI.

Before a device can be removed from the ECDS network, the following conditions must be met:

- Device must have been activated in the ECDSM.
- ECDSM must be operating.
- Device must have the correct ECDSM IP address or hostname configured.
- ECDSM IP address or hostname must be that of the primary ECDSM.



- Device must not be the Content Acquirer for any delivery service.

Deleting a device from the ECDS network involves using the CLI to remove the registration information from the device itself and removing the registration record from the ECDSM.

**Note**

Do not use the ECDSM to delete a device while the device is still active and registered. The ECDSM delete feature removes only the device's registration record from the ECDSM; it does not deregister the device. The device retains its registration information and continues to contact the ECDSM; however, the ECDSM no longer recognizes the device.

If for some reason the ECDSM loses the registration record of a device, use the **cms deregister force** command on the device to remove all its registration information. Then use the **cms enable** command to reregister the device with the ECDSM as though it were a new node in the ECDS network.

## Removing and Deregistering a Device Using CLI

To remove and deregister a device using CLI:

**Step 1** Open an SSH session to the device CLI.

**Step 2** In global configuration mode, enter the **no cms enable** command.

```
SE# configure
SE(config)# no cms enable
```

**Note**

Issuing the **no cms enable** command does not disable acquisition and distribution services on the device; however, issuing the **cms deregister** command does. The **cms deregister** command disables the CMS, all acquisition and distribution services, and all routing communications to and from this device.

**Step 3** In EXEC mode, enter the **cms deregister** command.

```
SE(config)# exit
SE# cms deregister
```

**Note**

The **cms deregister** command cleans up the database automatically. You do not need to use the **cms database delete** command.

If the deregistration fails, the best practice is to resolve any issues that caused the deregistration failure; for example, the Service Engine is the Content Acquirer of a delivery service and cannot be deleted or deactivated. In this case, assign a different SE as the Content Acquirer in each delivery service where this SE is assigned as the Content Acquirer and try the **cms deregister** command again.

**Step 4** If for some reason the deregistration fails, you can force the deregistration by using the **cms deregister force** command.

```
SE# cms deregister force
```

**Note**

Take note of any messages stating that the deregistration failed and make sure to resolve them before reregistering the device with the same ECDSM or registering the device to another ECDSM. The **cms deregister force** command forces the deregistration to continue.

- Step 5** To add the device back into the ECDS network, reregister the device with the ECDSM by using the **cms enable** command in global configuration mode.

```
SE# configure
SE(config)# cms enable
```

## Removing a Device with ECDSM

In case of a hardware failure, you might need to remove the device from the ECDS network routing scheme by using the ECDSM.

### Before You Begin

Before a device can be removed from the ECDS network through the ECDSM, the following conditions must be met:

- Device must have been activated in the ECDSM.
- ECDSM must be running.
- Device must have the correct ECDSM IP address or hostname configured.
- ECDSM IP address or hostname must point to the primary ECDSM.
- Device must not be the Content Acquirer for any delivery service.

### Procedure

To delete a device using the ECDSM:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed. The online status of the device is listed in the Status column.
- Step 2** Click the **Edit** icon next to the device name you want to delete. The Devices home page is displayed.
- Step 3** In the task bar, click the **Delete Device** icon. You are prompted to confirm your decision.
- Step 4** To execute your request, click **OK**. The device is removed from the ECDSM.
- Step 5** If possible, access the device CLI to deregister the device.
- Step 6** In the CLI, enter the **cms deregister force** command.

**Note**

You must use the **cms deregister force** command after deleting a device in the ECDSM. This is because once the device has been deleted, the ECDSM no longer has a record of the device.

- Step 7** To add the device back in to the ECDS network, reregister the device with the ECDSM by using the **cms enable** command in global configuration mode.

## Deleting a Warm Standby ECDSM

You can delete a warm standby ECDSM from the ECDS network at any point after you have registered the device and before the device has come online as the primary ECDSM. Once the device has been called into use as the primary ECDSM, however, you cannot delete it by using the ECDSM.

Delete a warm standby ECDSM when the device is experiencing unresolvable problems or when its network address or configuration has changed and you need to add the device back to the ECDS network by using its new address and configuration information.

To delete a warm standby ECDSM:

- 
- Step 1** Log in directly to the ECDSM CLI, and enter the **cms deregister** command.
- If for some reason the deregistration fails, you can force the deregistration by using the **cms deregister force** command.
- Step 2** From the ECDSM GUI, choose **Devices > Devices**.
- The browser refreshes, listing the ECDSMs on your ECDS network. The warm standby ECDSM is identified as *Standby*.
- Step 3** Click the **Edit** icon next to the name of the warm standby ECDSM. The Devices home page is displayed.
- Step 4** From the left-pane menu, choose **Device Activation**. The Activation page is displayed.
- Step 5** In the task bar, click the **Delete** icon. You are prompted to confirm your decision.
- Step 6** To execute your request, click **OK**.
- 

## Replacing a Device

The procedure to replace a device in the ECDS is different depending on the type of the device being replaced. This section covers the following procedures:

- [Replacing a ECDSM](#)
- [Replacing an SE or SR](#)

## Replacing a ECDSM

To replace a ECDSM in an ECDS you must first add the new ECDSM into the network as a standby ECDSM. For procedural information, see the [“Configuring Primary and Standby Enterprise CDSMs” section on page 3-11](#).



### Note

The primary and standby ECDSMs must be running the same version of software. You must first add the new ECDSM with the same version as the existing ECDSM. Once the standby ECDSM has been added, you must wait at least two polling intervals (10 minutes) for the databases to synchronize before you can begin the upgrade procedure.

**Note**

After you have activated the standby ECDSM using the primary ECDSM web interface and the device shows as online in the Devices Table page, wait at least two polling intervals (10 minutes) before changing roles to ensure that the standby ECDSM has a record of the most recent configuration changes.

To promote the standby ECDSM to primary, first stop the primary ECDSM using the **cdsm role standby** command. For procedural information, see the [“Changing a Standby to a Primary Enterprise CDSM” section on page 3-12](#).

After the primary ECDSM has been stopped, and the standby ECDSM has taken the role of primary, wait at least two polling intervals (10 minutes) before logging in to the new primary ECDSM. The new primary ECDSM is accessible by entering the IP address of the ECDSM with port 8443 in a web browser. For example, if the IP address of your ECDSM is 192.168.0.236, enter **https://192.168.0.236:8443**.

It is now safe to deactivate the old primary ECDSM in the ECDSM web interface and remove it from the ECDS network.

**Note**

Do not try to take a back up of the old ECDSM database and restore it on the new ECDSM. This may lead to problematic issues.

## Replacing an SE or SR

**Note**

If you replace a Content Acquirer with an SE that was not previously assigned to the delivery service, all content is reacquired and old content is deleted.

**Note**

To prevent the reacquisition of content when replacing a Content Acquirer, make one of the receiver SEs in the same delivery service the replacement Content Acquirer. Add the new SE as a receiver SE, wait until replication is complete for the newly added SE, and then designate it as the Content Acquirer. When you replace a Content Acquirer in this manner, the SEs in the delivery service synchronize with the new Content Acquirer through the metadata poll. Content is not redistributed to the other SEs in the delivery service unless the content has changed since the last metadata poll.

To replace an SE or SR:

- Step 1** Open an SSH session to the device being replaced.
- Step 2** In global configuration mode, enter the **no cms enable** command to disable CMS on the device that needs to be replaced.  

```
SE# configure
SE(config)# no cms enable
```
- Step 3** From the ECDSM, choose **Devices > Devices > Device Activation**. The Device Activation page is displayed.
- Step 4** Uncheck the **Activate** check box and click **Submit**. The page refreshes and displays a **Replaceable** check box.
- Step 5** Check the **Replaceable** check box and click **Submit**.
- Step 6** Choose **System > Configuration > System Properties**. The System Properties page is displayed.

- Step 7** Click the edit icon next to the **System.device.recovery.key** property. The Modify Config Property page is displayed.
- Step 8** In the **Value** field, enter a key and click **Submit**. The default value is default.
- Step 9** Follow the instructions for configuring a device using the setup utility. The instructions can be found in the [Cisco ECDS 2.5 Quick Start Guide](#).



**Note** The replacement device must be the same hardware model as that of the device being replaced.

- a. When prompted by the setup utility, configure the basic network settings.
- b. When prompted by the setup utility for the hostname of the new device, use the same hostname of the device being replaced. For example, if the old device has a hostname of “SE1,” the new device must have a hostname of “SE1.”
- c. When prompted by the setup utility for the IP address of the ECDSM, enter the IP address of the ECDSM.

**Step 10** Open an SSH session to the new device.

**Step 11** In EXEC mode, enter the **cms recover identity** command with the key parameter you set in [Step 8](#).

```
SE# cms recover identity <key>
```

On successful registration to the ECDSM, a message similar to the following is displayed:

```
DT-7326-4#cms recover identity sr
Registering this node as Service Router...
Sending identity recovery request with key sr
Node successfully registered with id CrConfig_291
Registration complete.
```

**Step 12** Register the device with the ECDSM by using the **cms enable** command in global configuration mode.

```
SE# configure
SE(config)# cms enable
```

**Step 13** From the ECDSM, choose **Devices > Devices > Device Activation**. The Device Activation page is displayed.

**Step 14** Check the **Activate** check box and click **Submit**.

After a few minutes, approximately two polling intervals, the device status shows online and all configurations (delivery service assignments, programs, and so on) are the same as those on the device that was replaced.

**Step 15** Once the new device is up and running, as noted by the online status, the old device can be removed from the ECDS network.

# Backup and Recovery

This section provides ECDSM database backup and ECDS software recovery procedures. This section contains the following sections:

- [Performing Backup and Restore on the ECDSM Database, page 11-16](#)
- [Recovering a Lost Administrator Password, page 11-17](#)
- [Recovering ECDS Network Device Registration Information, page 11-18](#)

## Performing Backup and Restore on the ECDSM Database

The ECDSM stores ECDS network-wide device configuration information in its Centralized Management System (CMS) database. You can manually back up the CMS embedded database contents for greater system reliability.

To back up the CMS database for the ECDSM, use the **cms database backup** EXEC command.



### Note

The naming convention for backup files includes the timestamp.

To back up and restore the CMS database on the ECDSM:

#### Step 1 Back up the CMS database to a file.

```
MDE# cms database backup
creating backup file backup-db-11-06-2007-13-10.dump
backup file local1/backup-db-11-06-2007-13-10.dump is ready.
Please use 'copy' commands to move the backup file to a remote host.
```

#### Step 2 Save the file to a remote server by using the **copy disk ftp** command. This command copies the file from the local disk to a remote FTP server, as shown in the following example:

```
MDE# cd /local1
MDE# copy disk ftp 10.86.32.82 /incoming cds-db-9-22-2002-17-36.dump
cds-db-9-22-2002-17-36.dump

Enter username for remote ftp server:ftp
Enter password for remote ftp server:*****
Initiating FTP upload...
Sending:USER ftp
10.86.32.82 FTP server (Version wu-2.6.1-18) ready.
Password required for ftp.
Sending:PASS *****
User ftp logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (10,86,32,82,112,221)
Sending:CWD /incoming
CWD command successful.
Sending: PASV
Entering Passive Mode (10,86,32,82,203,135)
Sending:STOR cds-db-9-22-2002-17-36.dump
Opening BINARY mode data connection for cds-db-9-22-2002-17-36.dump.
Transfer complete.
Sent 18155 bytes
```

- Step 3** Delete the existing CMS database.
- ```
MDE# cms database delete
```
- Step 4** Restore the CMS database contents from the backup file.
- ```
MDE# cms database restore cds-db-9-22-2002-17-36
```
- Step 5** Enable CMS.
- ```
MDE# cms enable
```
-

Recovering a Lost Administrator Password

If an administrator password is forgotten, lost, or misconfigured, reset the password on the device.



Note

There is no way to restore a lost administrator password. You must reset the password to a new one, as described in this procedure.

To reset the password:

- Step 1** Establish a console connection to the device and open a terminal session.
- Step 2** Reboot the device.
- While the device is rebooting, watch for the following prompt and press **Enter** when you see it:
- ```
Cisco CDS boot:hit RETURN to set boot flags:0009
```
- Step 3** When prompted to enter bootflags, enter the **0x800** value.
- ```
Available boot flags (enter the sum of the desired flags):
0x0000 - exit this menu and continue booting normally
0x2000 - ignore Carrier Detect on console
0x4000 - bypass nvram config
0x8000 - disable login security

[SE boot - enter bootflags]:0x8000
You have entered boot flags = 0x8000
Boot with these flags? [yes]:yes

[Display output omitted]
Setting the configuration flags to 0x8000 lets you into the system, bypassing all
security. Setting the configuration flags field to 0x4000 lets you bypass the NVRAM
configuration.
```
- Step 4** When the device completes the boot sequence, you are prompted to enter the username to access the CLI. Enter the default administrator username (**admin**).
- ```
Cisco Service Engine Console

Username: admin
```
- Step 5** When you see the CLI prompt, set the password for the user using the **username password** command in global configuration mode.
- ```
ServiceEngine# configure
ServiceEngine(config)# username admin password 0 password
```

You can specify that the password be either clear text or encrypted. Zero (0) means the password is displayed as a plain word; one (1) means the password is encrypted. The password strength must be a combination of alphabetic character, at least one number, at least one special character, and at least one uppercase character.



Note Do not set the user ID (uid).

Step 6 Save the configuration change by using the **write memory** command in EXEC mode.

```
ServiceEngine(config)# exit
ServiceEngine# write memory
```

Step 7 Optionally, reboot your device by using the **reload** command.

```
ServiceEngine# reload
```

Rebooting is optional; however, you might want to reboot to ensure that the boot flags are reset, and to ensure that subsequent console administrator logins do not bypass the password check.



Note In ECDS software, the bootflags are reset to 0x0 on every reboot.

Recovering ECDS Network Device Registration Information

Device registration information is stored both on the device itself and on the ECDSM. If a device loses its registration identity or needs to be replaced because of hardware failure, the ECDS network administrator can issue a CLI command to recover the lost information or, in the case of adding a new device, assume the identity of the failed device.

To recover lost registration information, or to replace a failed node with a new one having the same registration information:

Step 1 Mark the failed device as “Inactive” and “Replaceable” in the ECDSM:

- a. Choose **Devices > Devices**.
- b. Click the **Edit** icon next to the name of the Service Engine you want to deactivate. The Devices home page is displayed.
- c. From the left-panel menu, choose **Device Activation**.
- d. Uncheck the **Activate** check box. The page refreshes, displaying a check box for marking the device as replaceable.
- e. Check the **Replaceable** check box and click **Submit**.



Note This check box only displays when the device is inactive.

Step 2 Configure a system device recovery key:

- a. Choose **System > Configuration**.

- b. Click the **Edit** icon next to the `System.device.recovery.key` property. The Modifying Config Property page is displayed.
- c. Enter a password in the **Value** field and click **Submit**. The default password is **default**.

Step 3 Configure the basic network settings for the new device.

Step 4 Open an SSH session to the device CLI and enter the **cms recover identity keyword EXEC** command, where *keyword* is the device recovery key that you configured in the ECDSM.

When the ECDSM receives the recovery request from the Service Engine, it searches its database for the Service Engine record that meets the following criteria:

- Record is inactive and replaceable.
- Record has the same hostname as given in the recovery request.
- Device is the same hardware model as the device in the existing record.
- File system allocations for the device are the same as or greater than the device in the existing record.

If the recovery request matches the Service Engine record, then the ECDSM updates the existing record and sends the requesting Service Engine a registration response. The replaceable state is cleared so that no other device can assume the same identity. When the Service Engine receives its recovered registration information, it writes it to file, initializes its database tables, and starts.

Step 5 Return to the ECDSM and activate the device.

- a. Choose **Devices > Devices**.
- b. Click the **Edit** icon next to the name of the Service Engine you want to activate. The Devices home page is displayed.
- c. From the left-panel menu, choose **Device Activation**. The Service Engine status should be Online.
- d. Check the **Activate** check box and click **Submit**.

Disk Maintenance

This section describes the following maintenance tasks:

- [Disk Latent Sector Error Handling, page 11-19](#)
- [Removing and Replacing Hard Disk Drives, page 11-20](#)
- [Removing Content, page 11-21](#)

Disk Latent Sector Error Handling

Latent Sector Errors (LSEs) are when a particular disk sector cannot be read from or written to, or when there is an uncorrectable ECC error. Any data previously stored in the sector is lost. There is also a high probability that sectors in close proximity to the known bad sector have as yet undetected errors, and therefore are included in the repair process.

The syslog file shows the following disk I/O error message and smartd error message when there are disk sector errors:

```
Apr 28 21:00:26 U11-MDE1100-2 kernel: %SE-SYS-4-900000: end_request: I/O error, dev sdd,
sector 4660
```

```
Apr 28 21:00:26 U11-MDE1100-2 kernel: %SE-SYS-3-900000: Buffer I/O error on device sdd,
logical block 582
Apr 28 21:04:54 U11-MDE1100-2 smartd[7396]: %SE-UNKNOWN-6-899999: Device: /dev/sdd, SMART
Prefailure Attribute: 1 Raw_Read_Error_Rate changed from 75 to 73
Apr 28 21:04:54 U11-MDE1100-2 smartd[7396]: %SE-UNKNOWN-6-899999: Device: /dev/sdd, SMART
Usage Attribute: 187 Reported_Uncorrect changed from 99 to 97
Apr 28 21:04:54 U11-MDE1100-2 smartd[7396]: %SE-UNKNOWN-2-899999: Device: /dev/sdd, ATA
error count increased from 1 to 3
```

The **disk repair** command repairs the bad sector, including the proximal sectors and then reformats the drive. All data on the drive is lost, but the sectors are repaired and available for data storage again.



Caution

The device should be offline before running the **disk repair** command. Because this command involves complex steps, we recommend you contact Cisco Technical Support before running it.

The **disk repair** command not only repairs the bad sectors, but reformats the entire drive, so all data on the drive is lost. The difference between the **disk repair** command and the **disk reformat** command is that the **disk format** command only reinitializes the file system and does not repair bad sectors.

The **disk repair** command has the following syntax:

```
# disk repair disk_name sector sector_address_in_decimal
```

For example, the following command repairs the sector 4660 on disk 02:

```
# disk repair disk02 sector 4660
```

A minor alarm is set when an LSE is detected. After the sector is repaired with the **disk repair** command, the alarm is turned off.

Minor Alarms:

```
-----
Alarm ID           Module/Submodule   Instance
-----
1 badsector        sysmon            disk11
May 19 20:40:38.213 UTC, Equipment Alarm, #000003, 1000:445011
"Device: /dev/sd1, 1 Currently unreadable (pending) sectors"
```

For information about disk error handling, see the [“Setting Storage Handling” section on page 5-76](#).

Removing and Replacing Hard Disk Drives

To replace a disk, simply power down the unit, remove the disk, insert the new disk, and reboot. During the reboot, the system automatically detects any new disks and seamlessly allocates their space according to a simple disk-policy heuristic.

The disk policy’s design, when adding new disks, is to always favor safety. When a new disk is added, the disk manager detects “degraded” or “bad” system file system (sysfs) volumes, the new disk is used to repair the sysfs volumes. Thus, the disk manager always strives to have two disks allocated to the sysfs volumes. When a new disk is added, the sysfs volumes are “normal” or “syncing,” the new disk is added to the cdnfs volume.

For more information about removing and inserting hard disk drives, see the following documents:

- [Cisco MDE 1100 Appliance Hardware Installation Guide](#)
- [Cisco MDE 3100 Appliance Hardware Installation Guide](#)

Removing Content

The Content Removal page allows you to delete content manually, either by referencing a single URL or by using an XML file for batch deletions.

- [Single Content Removal, page 11-21](#)
- [Batch Content Removal, page 11-21](#)

Single Content Removal

To delete content manually:

-
- Step 1** Choose **Services > Service Definition > Delivery Service**. The Delivery Services Table page is displayed
 - Step 2** Click the **Edit** icon next to the delivery service name that has the content you want to delete.
 - Step 3** Choose **Tools > Content Management**. The Content Removal page is displayed.
 - Step 4** In the **URL String** field for a single URL removal, enter the URL of the content you want to remove. Click **Help** for an example.
 - Step 5** Click **Submit**.
-

Batch Content Removal

The batch content removal uses an XML file that lists the URLs of the content to delete. The XML batch content removal file can be created with any ASCII text editing tool.

The XML Schema file describes and dictates the content of the XML file. The URLRemoval.xsd file contains the XML schema.

The following code is the URL Removal XML schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:cds-ns="http://cisco.com/unicorn/cds/urlmgmt"
  targetNamespace="http://cisco.com/unicorn/cds/urlmgmt"
  xmlns="http://cisco.com/unicorn/cds/urlmgmt"
  elementFormDefault="qualified">

  <xsd:element name="URLRemovalList">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="url-entry" minOccurs="1" maxOccurs="unbounded" type="xsd:string" />
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>

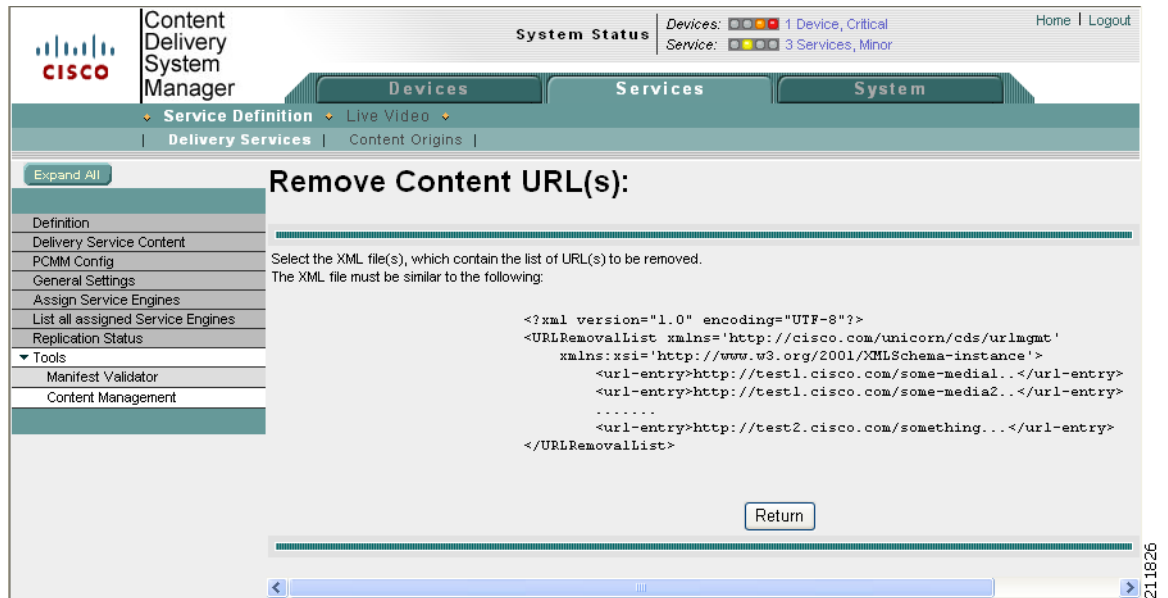
</xsd:schema>
```

To delete content items in a batch:

-
- Step 1** Create an XML file containing the URLs of the content you want to delete by using the XML example shown in the Content Removal—Batch File Help page.

Figure 11-2 shows the URL Removal XML file example displayed when you click **Help**.

Figure 11-2 Content Removal—Batch File Help Page



Step 2 In the **Batch File** field for a Batch URL removal, enter the URL of the XML file.

Step 3 Click **Submit**.

Where to Go Next

For the most current ECDS hardware and software support information, see the [Cisco ECDS 2.5 Release Notes](#) and the Cisco ECDS 2.5 Software Administration Configuration Guide.



APPENDIX **A**

Troubleshooting

The following sections describe how to troubleshoot the ECDS:

- [Troubleshooting Tips for the CDSM, page A-1](#)
- [Troubleshooting Service Router Configurations, page A-2](#)
- [Verifying and Troubleshooting the Service Engine, page A-3](#)
- [Verifying and Troubleshooting WCCP, page A-3](#)
- [Troubleshooting the Distribution Hierarchy, page A-8](#)
- [Troubleshooting Content Acquisition, page A-10](#)
- [Enabling the Kernel Debugger, page A-13](#)
- [Where to Go Next, page A-14](#)



Tip

For more troubleshooting tools, see [Chapter 10, “Monitoring the Enterprise CDS.”](#)

Troubleshooting Tips for the CDSM

If your CDSM has been running for a long time without a reboot, some devices may appear to be offline or may not reflect updated settings. Reboot the CDSM to bring SEs back to an online and current state.

Troubleshooting Service Router Configurations

Because there are many steps required for the Service Router to redirect the request properly, you might see some content request errors from the Service Router when the configuration is not quite complete.

[Table A-1](#) suggests troubleshooting tips:

Table A-1 *Service Router Configuration Troubleshooting Tips*

Check For	Description	Where to Go Next
DNS delegation	Is the requested domain delegated to the Service Router on the DNS server that is authoritative for the parent domains? The Service Router's DNS name should be forward resolvable.	Check with the system administrator to delegate a domain.
Service Router routing properties	Is the Service Router activated?	“Activating a Service Router” section on page 6-1 to activate a Service Router.
	Is a default coverage zone set for a Service Engine, or is there an ECDS network-wide Coverage Zone file or a local Coverage Zone file set for the Service Router?	“Coverage Zone File Registration” section on page 9-11 to set a Coverage Zone file. “Configuring the Enterprise CDSM” section on page 4-9 to set a default coverage zone.
	Is the content request from an end system covered by a Service Engine in a coverage zone based on the default coverage zone or the Coverage Zone file? This Service Engine is the “serving Service Engine.”	“Coverage Zone File” section on page 1-23 for information on coverage zones. Appendix C, “Creating Coverage Zone Files,” for information on creating a Coverage Zone file.
	Is the serving Service Engine activated?	“Activating a Service Engine” section on page 5-1 to activate a Service Engine.
	Is there a delivery service created for the requested domain and a serving Service Engine assigned to this delivery service?	“Creating Delivery Service” section on page 8-4.
	Is the serving Service Engine alive? Use the show statistics service-routing se command to show the status of a Service Engine.	“Using the CDSM Show/Clear Commands Tool” section on page 10-12.

Tip For general information, use the **show statistics service-router all** command.

Verifying and Troubleshooting the Service Engine

Table A-2 **Service Router Configuration Troubleshooting Tips**

Check For	Description	Where to Go Next
Devices in SE device groups.	Once the configuration is successfully set for a device group, the system displays the intended configuration of the entire device group rather than the status of individual devices within the group in the ECDS administration GUI.	Verify that all devices within your device group are successfully configured by running the show config commands for each device on the Service Engine. If any error is found on the device using the CLI, reconfigure that device by returning to the ECDS administration GUI. Any subsequent changes that you make to your Service Engine configuration should be verified using the CLI and corrected using the ECDS administration GUI.
Content prefetched on a Service Engine	Is a Manifest file assigned to the delivery service associated with the serving Service Engine?	“Working with Manifest Files” section on page B-2.
	Is the Manifest file accessible from the CDSM?	“Identifying Content Using a Manifest File” section on page 8-21.
	Is there any syntax error in the Manifest file?	“Manifest File Structure and Syntax” section on page B-19.
	Is the requested content specified in the Manifest file?	“Specifying a Single Content Item” section on page B-3.
	If the requested content is streaming media, is the protocol engine enabled?	“Application Control” section on page 5-22.
NTP configuration	When configuring network settings on your Service Engine in the ECDS administration GUI.	Make sure that you configure NTP in General Settings > Network > NTP and enter the ntp server <ntp-server-IP> command. This enables the Service Engine to work properly with Flash Media Streamer and successfully sync with CDSM.

Verifying and Troubleshooting WCCP

The following sections describe commands and debugging methods that will help you and Cisco technical support manage any WCCP issues. For complete command details, see the [Cisco ECDS Command Reference](#).

- [Show Commands, page A-4](#)
- [Debug Commands, page A-6](#)
- [GRE Packet Capture Commands, page A-8](#)
- [WCCP Logging, page A-8](#)
- [WCCP Logging Examples, page A-8](#)

Show Commands

Table A-3 lists available **show** commands to troubleshoot your WCCP configuration. Trace the messages corresponding to the debug option enabled in WCCP Log File.

```
ServiceEngine# show wccp ?
```

Table A-3 WCCP Show Commands

Keyword	Description
flows	WCCP packet flow information.
gre	Running status of WCCP GRE counters.
masks	WCCP mask assignments.
modules	Running status of WCCP registered modules.
masks	
modules	
port-list	Running status of WCCP port-lists.
routers	WCCP router list.
service-engines	WCCP service engine information; verify successful connection.
services	WCCP configured services information.
slowstart	WCCP slow start information. Slow start mode: Tracking.
status	WCCP running status

Show Command Examples

Example A-1 WCCP Services

```
ServiceEngine# show wccp services detail
```

```
Service Details for Web Cache Service
  Service Enabled           : Yes
  Service Priority          : 240
  Service Protocol         : 6
  Application               : Caching
  Service Flags (in Hex)   : 512
  Service Ports             :      80      0      0      0
                           :      0      0      0      0
  Security Enabled for Service : No
  Multicast Enabled for Service : No
  Weight for this Web-SE     : 0
  Negotiated forwarding method : L2
  Negotiated assignment method : MASK
Received Values:
  Source IP mask (in Hex)    : 12
  Destination IP mask (in Hex) : 12
  Source Port mask (in Hex)  : 1
  Destination Port mask (in Hex) : 1
Calculated Values:
  Source IP mask (in Hex)    : 12
  Destination IP mask (in Hex) : 12
```



```

Source Port mask (in Hex)      : 1
Destination Port mask (in Hex) : 1

Service Details for Reverse Proxy Service
Service Enabled                : No
Service Priority                : 0
Service Protocol               : 0
Application                    : Unknown
Service Flags (in Hex)         : 500
Service Ports                  :      0      0      0      0
                              :      0      0      0      0

Security Enabled for Service   : No
Multicast Enabled for Service  : No
Weight for this Web-SE         : 0
Negotiated forwarding method   : GRE
Negotiated assignment method   : HASH
Received Values:
Source IP mask (in Hex)        : 0
Destination IP mask (in Hex)    : 0
Source Port mask (in Hex)       : 0
Destination Port mask (in Hex)  : 0
Calculated Values:
Source IP mask (in Hex)         : 0
Destination IP mask (in Hex)    : 1741
Source Port mask (in Hex)       : 0
Destination Port mask (in Hex)  : 0

```

Example A-2 HTTPS Configuration

The following example displays all HTTPS configuration parameters:

```

ServiceEngine# show https all
Incoming HTTPS proxy:
Incoming Proxy-Mode:
    Not servicing incoming proxy mode connections.
Outgoing HTTPS proxy:
Outgoing Proxy-Mode:
    Not using outgoing proxy mode.

Monitor Interval for Outgoing Proxy Servers is 60 seconds

Timeout period for probing Outgoing Proxy Servers is 300000 microseconds

Use of Origin Server upon Proxy Failures is disabled.
Destination port restrictions:
Allow 443 563
HTTPS caching certificate information:
  1. Certificate Name : d
     Subject : <empty>

HTTPS caching certificate group information:
HTTPS caching private key information:
  1. Private Key Name : key1
     Attributes : <empty>

Display all https server caching information:
  1: name name, host <not configured>, disabled
ServiceEngine#

```

The following example displays the HTTPS proxy configuration details:

```

ServiceEngine# show https proxy
Incoming HTTPS proxy:
Incoming Proxy-Mode:

```

```

Configured Proxy mode HTTPS connections on ports: 9090
Outgoing HTTPS proxy:
Outgoing Proxy-Mode:

Primary Proxy Server:          10.77.155.221 port 8088 Failed

Monitor Interval for Outgoing Proxy Servers is 20 seconds

Timeout period for probing Outgoing Proxy Servers is 3000 microseconds

Use of Origin Server upon Proxy Failures is enabled.
ServiceEngine#

```

Debug Commands

For complete command details, see the [Cisco ECDS Command Reference](#)

- [Router Debug Commands, page A-6](#)
- [Debug Command Examples, page A-6](#)

Service Engine Debug Commands

[Table A-4](#) lists debugging commands that are available in the SE for WCCP.

```
ServiceEngine# debug wccp ?
```

Table A-4 WCCP Service Engine Debug Commands

Keyword	Description
all	Turns on all WCCP debugging.
detail	Detailed information about WCCP.
error	WCCP error information.
events	WCCP events.
keepalive	WCCP keepalive to applications.
packets	WCCP packet-related information
slowstart	WCCP slow start information.

Router Debug Commands

[Table A-5](#) lists available Cisco router debug commands.

Table A-5 Cisco Router Debug and Show Commands

Command Line	Description
debug ip wccp events	Debugs WCCP events.
debug ip wccp packets	Debugs WCCP packet-related information.

Debug Command Examples

The following example turns on debugging for WCCP packet diagnostics:

Example A-3 WCCP Events

```
Router# debug ip wccp event
```

WCCP events debugging is on

Example A-4 WCCP Packets

```
Router# debug ip wccp packet
```

WCCP packet info debugging is on

```
Router#
2d18h: WCCP-EVNT:S00: Built new router view: 0 routers, 0 usable web caches, change #
00000001
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000001
2d18h: WCCP-EVNT:S00: Redirect_Assignment packet from 192.168.15.2 fails source check
2d18h: %WCCP-5-SERVICEFOUND: Service web-cache acquired on Web Cache 192.168.15.2
2d18h: WCCP-PKT:S00: Received valid Here_I_Am packet from 192.168.15.2 w/rcv_id 00000001
2d18h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change #
00000002
```

Example A-5 Enable/Disable Debug Trace

```
SE1# debug wccp all
SE1# show debug
```

```
Debug Authsvr error is on
Debug wccp all is On
Debug wccp detail is On
Debug wccp error is On
Debug wccp events is On
Debug wccp keepalive is On
Debug wccp packets is On
Debug wccp slow-start is On
```

```
SE1# undebug all
SE1# show debug
```

```
Debug wccp all is On
Debug wccp detail is On
Debug wccp error is On
Debug wccp events is On
Debug wccp keepalive is On
Debug wccp packets is On
Debug wccp slow-start is On
```

Example A-6 Trace Error Logs

Enable WE debug trace in error logs:

```
U10-2G2-5# debug web-engine trace
U10-2G2-5# web-engine debug-module all
```

Example A-7 Transaction and Ingest Logging

Enable the transaction logging & ingest logging for debugging:

```
U10-2G2-5(config)# transaction-logs enable
U10-2G2-5(config)# transaction-logs format extended-squid
U10-2G2-5(config)# web-engine http-ingest-logging enable
U10-2G2-5(config)# end
```

GRE Packet Capture Commands

Capture GRE packets with the **tcpdump** command. [Table A-6](#) lists available **tcpdump** commands.

Table A-6 GRE Packet Capture Commands

Command Line	Description
tcpdump proto 47	Captures all GRE traffic.
tcpdump proto 47 or port 80	Captures all web cache and GRE traffic.
tcpdump proto 47 or port 1935	Captures all RTMP and GRE traffic.

WCCP Logging

All WCCP logs are found in the following location:

/local/local1/service_logs

In the SE:

-
- Step 1** CD to /local/local1/service_logs.
- Step 2** Enter **ls -l wccp***.
- All available WCCP logs are displayed.
-

WCCP Logging Examples

Example A-8 Q-String Caching

The following examples check Web Engine extended logs & ingest logging.

```
webengine# type-tail /local1/logs/webengine_extsquid/working.log
```

```
[12/Jul/2012:16:00:31.937-0700] 2815644 3.1.7.105 TCP_MISS/200 7951 GET
http://2.225.2.68/we/tmp/raji-225.html?name=rajirajiabcdefghijkmnaopqrstuvabcdefghijkmnopqrs
tuvwsxy text/html;charset=UTF-8
```

```
[12/Jul/2012:16:00:31.952-0700] 2800771 3.1.7.100 TCP_HIT/200 7951 GET
http://2.225.2.68/we/tmp/raji-225.html?name=rajirajiabcdefghijkmnaopqrstuvabcdefghijkmnopqrs
tuvwsxy text/html;charset=UTF-8
```

```
U10-2G2-5# type-tail /local1/logs/webengine_ingestlog_clf/working.log
```

```
[12/Jul/2012:16:01:51-0700]
http://2.225.2.68/we/tmp/raji-441.html?name=rajirajiabcdefghijkmnaopqrstuvabcdefghijkmnopqrs
tuvwsxy 3.1.7.21/3.1.7.9/2.225.2.68/ 3.1.7.21 7688 7688 7688 100 0 200 text/html;
charset=UTF-8 No 2.225.2.68
```

Troubleshooting the Distribution Hierarchy

Because distribution-related problems are design-dependent, your initial strategy is to discover whether or not the correct Service Engine is sending content in the correct distribution path:

- [Determining the Distribution Path, page A-9](#)
- [Determining Reachability and Hierarchy, page A-9](#)

Determining the Distribution Path

To determine which Service Engines are in the distribution path of a particular Service Engine, use the **show distribution remote traceroute EXEC** command, as shown in the following example:

```
se1# show distribution remote traceroute ?
forwarder-next-hop  next forwarder along the path
unicast-sender       check status for unicast sender

se1# show distribution remote traceroute forwarder-next-hop ?
delivery-service-id  Delivery-service-id of a Delivery Service

se1# show distribution remote traceroute forwarder-next-hop delivery-service-id 133 ?
max-hop              Trace route till specified number of hops is reached
trace-till-good      traceroute till probe is good or the object is found
trace-till-root       traceroute till the acquirer

se1# show distribution remote traceroute forwarder-next-hop delivery-service-id 133
trace-till-root
```

Hop	NextHop_SEId	NextHop_SEName	NextHop_SEIp	GenID	Status/Reason
1	1100	ce3	10.255.0.43	1	LOC-LEAD
1	1100	ce3	128.107.193.183	1	LOC-LEAD (Reached RootSE)

Determining Reachability and Hierarchy

To verify that the Service Engine is reachable and that it is in the distribution hierarchy, use the **show distribution remote traceroute EXEC** command, as shown in the following example:

```
se1# show distribution remote traceroute unicast-sender delivery-service-id 133 ?
cdn-url             check the object on remote SE using cdn-url
probe               probe the remote unicast sender
relative-cdn-url    check the object on remote SE using relative-cdn-url

se1# show distribution remote traceroute unicast-sender delivery-service-id 133 probe ?
max-hop             Max-hop to traceroute to
trace-till-good     traceroute till probe is good or the object is found
trace-till-root     traceroute till the root se

se1# show distribution remote traceroute unicast-sender delivery-service-id 133 probe
trace-till-root
Polling .... se3 [10.255.0.43] Fwdr_Id:1100
Polling .... se3 [128.107.193.183] Fwdr_Id:1100
(Reached RootSE)
```

Troubleshooting Content Acquisition

To monitor acquisition progress and to troubleshoot, use commands from the Content Acquirer CLI to check the following:

[Delivery Services, page A-10](#)

[Acquirer Processes, page A-10](#)

[Acquirer Progress, page A-10](#)

[Detailed Acquisition Statistics, page A-11](#)

[Acquirer Errors, page A-11](#)

[Debug Acquirer, page A-11](#)

[Verify Pre-Positioning, page A-12](#)

[Verify Files on the Disk, page A-13](#)

Delivery Services

Use the **show acquirer delivery-services** EXEC command to obtain delivery service information, such as the delivery service ID and delivery service name, that you need to enter in other **show acquirer** commands, such as the **show acquirer progress** command. In the following example, the delivery service ID is 793 and the delivery service name is group01-cifs.

```
SE# show acquirer delivery-services
Querying Database.....
Acquirer information for all delivery services:
-----
Delivery-service-id       : 793
Delivery-service-Name     : group01-cifs
WebSite-Name             : group01-cifs
Root-SE-Type             : Configured
State                    : Enabled
Disk Quota                : 200 MB
Origin FQDN              : cdn.allcisco.com
Delivery-service Priority : 500
Manifestfile-TTL         : 5
Manifestfile-URL         : ftp://10.1.1.1/cifs.xml
```

Acquirer Processes

Use the **show acquirer** EXEC command to make sure that the acquirer process on the Content Acquirer is working correctly, and that the device is using the expected amount of bandwidth for acquisition. The following example shows that the acquirer is running properly and that the device is configured with unlimited bandwidth for acquisition of content.

```
SE# show acquirer
Acquirer is running OK
Current Acquisition Bandwidth:Not Limited
```

Acquirer Progress

Use the **show acquirer progress** EXEC command to check how far the acquisition of content has progressed. A specific delivery service ID or delivery service name can be specified to obtain the progress for a specific delivery service. In the following example, the acquirer has already acquired 2237 items.

```
SE# show acquirer progress delivery-service-id 793
Querying Database.....
```

```
Acquirer progress information for delivery service ID:793
Delivery-service-Name:group01-cifs
-----
```

```
Acquired Single Items      :          0 / 0
Acquired Crawl Items       :      2237 / 2500    -- start-url=www.mtv.com//
```

Detailed Acquisition Statistics

Use the **show statistics acquirer delivery-service-id** or **show statistics acquirer delivery-service-name** EXEC command to obtain the detailed acquisition statistics for a given delivery service. In the following example, there was an error acquiring two items.

```
SE# show statistics acquirer delivery-service-id 793
```

```
Querying Database.....
```

```
Statistics for Delivery Service Delivery-service-id :793 Delivery-service-Name
:group01-cifs
-----
```

```
Manifest:
-----
```

```
Fetch Errors      :0
Parsing Errors    :0
Parsing Warnings  :0
```

```
Acquisition:
-----
```

```
Total Number of Acquired Objects      :2237
Total Disk Used for Acquired Objects    :981511280 Bytes
Total Number of Failed Objects          :2
Total Number of Re-Check Failed Objects :0
```

Acquirer Errors

Use the **show statistics acquirer errors delivery-service-id** or **show statistics acquirer errors delivery-service-name** EXEC command to see the reasons why the errors occurred. In the following example, one error occurred because there was a problem acquiring the URL. The other error occurred because the disk quota for the delivery service configured in the Content Distribution Manager GUI would have been exceeded if the specified URL had been acquired. You can increase the delivery service disk quota to correct this error.

```
SE# show statistics acquirer errors delivery-service-id 793
```

```
Querying Database.....
```

```
Acquisition Errors for the Delivery Service ID:793
-----
```

```
Crawl job:start-url http://www.mtv.com//
Crawl Errors
-----
```

```
Internal Server Error(500):http://cgi.cnn.com/entries/intl-emailsubs-confirm
Exceeded Disk Quota(703):http://www.cdt.org/copyright/backgroundchart.pdf
```

Debug Acquirer

If more detailed troubleshooting of content acquisition is required, you can increase the debug level of the acquirer using the **debug acquirer trace** EXEC command. The logs are written to `local1/errorlog/acquirer-errorlog.current`.

Verify Pre-Positioning

To verify that an expected object has been pre-positioned on the Service Engine, use the **show distribution object-status EXEC** command, as shown in the following example. By comparing fields, such as Total Size, Transferred Size, and Source URL in the Object Replication output and Actual File Size and Source URL in the Source-URL to CDN-Object Mapping output, you can determine whether or not the object that is stored is the same as the object that was requested.

```
SE# show distribution object-status
http://172.18.81.168/Videos/SM-final%20Innebandy%202003.wmv

===== Website Information =====
Name: RTPServer5
Origin Server FQDN: 172.18.81.168
Service Routing FQDN: N/A
Content UNS Reference #: 1
===== Delivery Services Information =====
*** Delivery Service 1903 (name = A_Multicast) ***

Object Replication
-----
Replication: Done
File State: Ready for distribution
Multicast for Delivery Service: Not Enabled
Replication Lock: Received by Unicast-Receiver/Acquirer
Reference Count: 1
Total Size: 2756437
Transferred Size: 2756437
MD5 of MD5: tjs#DxqE5oUc024Z8XtFDw..
Source Url: http://172.18.81.168/Videos/SM-final%20Innebandy%202003.wmv
Source Last Modified Time: Wed Jan 7 19:03:48 2004

Object Properties
-----
Redirect To Origin: Yes
Requires Authentication: No
Alternative URL:
Serve Start Time: N/A
Serve End Time: N/A
Play servers: HTTP HTTPS WMT
Content Metadata: None
Content uns_id: NgcJTCU#JaY4ZGIPbsrONw..
Content gen-id: 1768:1136512329:2

===== CDNFS Information =====
Internal File Name:
/disk00-04/d/http-172.18.81.168-k5bsm1o+y14jgiqsvwaohq/19/19f6d5cec7266c33f419709dc28c8d9b
.0.data.wmv
Actual File Size: 2756437 bytes
MD5 of MD5 (Re-calculated): tjs#DxqE5oUc024Z8XtFDw..
Content metadata: None
Metadata match with: Delivery Service 1903
Number of Source-urls: 1

Source-url to CDN-object mapping:
Source-url: http://172.18.81.168/Videos/SM-final%20Innebandy%202003.wmv
Used by CDN object: ---- Yes ----
Internal File Name:
/disk00-04/d/http-172.18.81.168-k5bsm1o+y14jgiqsvwaohq/19/19f6d5cec7266c33f419709dc28c8d9b
.0.data.wmv
Actual File Size: 2756437 bytes

===== CDNFS lookup output =====
CDNFS File Attributes:
```



```

Status                3    (Ready)
File Size              2756437 Bytes
Start Time             null
End Time               null
Allowed Playback via   HTTP WMT HTTPS
Last-modified Time     Wed Jan 7 19:03:48 2004
cache-control          max-age=864000
cdn_uns_id             NgcJTCU#JaY4ZGIPbsrONw..
content-type           video/x-ms-wmv
etag                  "042e6fa50d5c31:b39"
file_duration          65
last-modified          Wed, 07 Jan 2004 19:03:48 GMT
server                 Microsoft-IIS/6.0
x-powered-by           ASP.NET
Internal path to data file:
/disk00-04/d/http-172.18.81.168-k5bsml0+y14jgiqsvwaohq/19/19f6d5cec7266c33f419709dc28c8d9b
.0.data.wmv

```

Verify Files on the Disk

To view the file directory structure on the Service Engine and verify the physical file on the disk, you can use the **cdnfs browse** EXEC command, as shown in the following example:

```
SE# cdnfs browse
```

```

----- CDNFS interactive browsing -----
dir, ls:    list directory contents
cd, chdir:  change current working directory
info:       display attributes of a file
more:       page through a file
cat:        display a file
exit,quit:  quit CDNFS browse shell

/>ls
                                srv2-static.cisco.com/
                                http-172.18.81.151-glfc4h-b9gywnf5rlnfweg/
                                http-172.18.81.163-og5o2lu178nrhwlmctgtiq/
                                172.18.81.163/
                                file--xrnfwxifgu62jtiwtyixvg/
                                172.18.81.168/
                                http-172.18.81.168-k5bsml0+y14jgiqsvwaohq/
                                172.18.81.155/

/>cd 172.18.81.168/
/172.18.81.168/>ls
376 Bytes          manifest-Delivery_service_1903.xml-1EYmrfnjt2o5GbUNwLCaPA
                   Videos/

/172.18.81.168/>cd Videos
/172.18.81.168/Videos/>ls
2756437 Bytes      SM-final Innebandy 2003.wmv <=====Physical file on disk
/172.18.81.168/Videos/>quit
SE#

```

Enabling the Kernel Debugger

Cisco ECDS software allows you to enable or disable access to the kernel debugger from the CDSM. Once enabled, the kernel debugger is automatically activated when kernel problems occur.



Note

The “hardware watchdog” is enabled by default and automatically reboots a device that has stopped responding for over ten minutes. Enabling the kernel debugger disables the “hardware watchdog.”

If the device runs out of memory and kernel debugger (KDB) is enabled, the KDB is activated and dump information. If the KDB is disabled and the device runs out of memory, the syslog reports only dump information and reboots the device.

To enable the kernel debugger:

-
- Step 1** Choose **Devices > Devices > General Settings > Troubleshooting > Kernel Debugger**. The Kernel Debugger page is displayed.
- Step 2** Check the **Enable** check box, and click **Submit**.
-

Where to Go Next

For the most current ECDS hardware and software support information, see the [Cisco ECDS 2.5 Release Notes](#) and the Cisco ECDS 2.5 Software Administration Configuration Guide.



APPENDIX **B**

Creating Manifest Files

The following sections describe the process for creating Manifest files, which acquire and distribute content within the ECDS network:

- [Introduction, page B-1](#)
- [Manifest File Requirements, page B-2](#)
- [Working with Manifest Files, page B-2](#)
- [Manifest Validator Utility, page B-15](#)
- [Manifest File Structure and Syntax, page B-19](#)
- [XML Schema, page B-46](#)
- [Manifest File Time Zone Tables, page B-52](#)



Tip

For information about using a Manifest file in a delivery service, see the ““Identifying Content Using a Manifest File” section on page 8-21 of Chapter 8, “Configuring Services.”.

Introduction

The ECDS is used to ingest, distribute, and deliver multi-format content to different client devices. To specify the content to be prefetched and to control the delivery of the prefetched content, an XML file called a *Manifest file* is used. Third-party asset management systems can interoperate with the ECDS by using this Manifest file interface. Each delivery service in the ECDS can be configured with or without a Manifest file. The Manifest file can also be automatically generated by using the CDSM. The Manifest file is primarily used in prefetch ingest and hybrid ingest.

The Manifest file is specified in the CDSM in the following ways:

- **External Manifest File Specification**—The Manifest file is hosted on an external server and a URL pointing to that server is configured in the delivery service. The Manifest file can be fetched using FTP, HTTP, HTTPS, and CIFS protocols.
- **GUI Configured**—The CDSM GUI can generate a Manifest file. The CDSM provides the required elements for the user to create a Manifest file and to specify the attributes in the Manifest file. Only commonly used attributes are supported by the CDSM.

The Manifest file is processed by the Content Acquirer. The Content Acquirer parses the Manifest file, creates the metadata based on the attributes in the file, and prefetches the content specified. For live content and content that is ingested on demand, the Content Acquirer creates the metadata and does not fetch the actual content. The metadata created by the Content Acquirer is propagated to all the Service Engines participating in the delivery service.

Manifest File Requirements

The Manifest file needs to support different attributes and tags to support content prefetching and hybrid ingest. The basic requirements for a Manifest file are as follows:

- **Specify Content to Be Prefetched**—There are two ways to specify prefetched content. One is to use a single item, where users specify a single URL and the Content Acquirer ingests only the content pointed to by this URL. Another way is by using a crawler item, where users specify a crawl job with parameters like start-url, depth, prefix, and reject or accept. In this case, the Content Acquirer crawls the origin server to fetch content based on the parameters.
- **Specify Schedule Information**—To instruct the Content Acquirer when to ingest the content and how often to check the server for updates.
- **Specify Publish Information**—Information about how content is accessed by the end users; for example, the playserver attribute specifies which server to use for playing the content, the cdn-url attribute specifies which URL is used by end-users to access the content, the *serveStartTime* and *serveStopTime* attributes instruct the ECDS when it can serve the content and provides additional metadata for playing.
- **Specify Live Streaming Content**—The Manifest file can also be used to specify live stream splitting.
- **Specify Metadata for Hybrid Ingest Content**—For hybrid ingest, the Manifest file can be used to specify the content serve start and stop time for content ingested on demand.

**Note**

In the current release, the origin server OFQDN is always used, and the hostname/port in the Manifest file is ignored.

Working with Manifest Files

This section provides Manifest file samples for specific scenarios. Each sample has an associated explanation of its purpose and function. The Manifest file can specify a single content object, a website crawler job, or an FTP server crawler job to acquire prefetched content or to acquire information about live content that is distributed to edge Service Engines later.

- [Specifying a Single Content Item, page B-3](#)
- [Specifying a Crawl Job, page B-4](#)
- [Understanding the Prefix Attribute, page B-6](#)
- [Writing Common Regular Expressions, page B-7](#)
- [Scheduling Content Acquisition, page B-7](#)
- [Specifying Shared Attributes, page B-7](#)
- [Specifying a Crawler Filter, page B-8](#)
- [Specifying Content Priority, page B-10](#)

- [Generating a Playserver List, page B-11](#)
- [Customized Manifest Playserver Tables and the HTTP Playserver, page B-11](#)
- [Specifying Attributes for Content Serving, page B-12](#)
- [Specifying Time Values in the Manifest File, page B-13](#)
- [Refreshing and Removing Content, page B-13](#)
- [Specifying Live Content, page B-14](#)
- [Specifying Hybrid Ingest Content, page B-15](#)

Specifying a Single Content Item

Use the `<item>` tag to specify a single content item, object, or URL. The required `src` attribute is used to specify the relative path portion of the URL. If the server *name* attribute is omitted, the server *name* attribute in the last specified `<server>` tag above it is used. If there are no `<server>` tags close by in the Manifest file, the server that hosts the Manifest file is used, which means that the relative URL is relative to the Manifest file URL.

[Example B-1](#) shows a Manifest file that specifies single content items.

Example B-1 Single Content Manifest File

```
<CdnManifest>
  <item src="http://www.my-server/test.html" />
  <item src="test.html" />
  <server name="my-origin-server-one">
    <host name="http://www.my-server-one.com/eng/" />
  </server>
  <server name="my-origin-server-two">
    <host name="http://www.my-server-two.com/eng/" />
  </server>
  <item src="project-two.html" />
  <item server="my-origin-server-one" src="project-one.html" />
</CdnManifest>
```

For a single item, specify the item's URL in the `src` attribute. There are two ways to specify the item URL:

- Specify the `src` attribute with the absolute URL as shown in the following format:

```
proto://username:password@/domain-name:port/file-path/file-name
```

In the example, the first `<item>` tag uses the full path.

- Specify the origin server information using the `<server>``<host>` tags and use the `src` attribute to specify only the relative path.

In the example, every `<item>` tag except the first one uses a relative path. The second `<item>` tag uses the Manifest file server, where `test.html` is relative to the Manifest file URL. The second `<item>` tag, “`project-two.html`,” uses “`my-origin-server-two`.” The third `<item>` tag, “`project-one.html`,” uses “`my-origin-server-one`.”

Specifying a Crawl Job

The crawler feature methodically and automatically searches acceptable websites and makes a copy of the visited pages for later processing. The crawler starts with a list of URLs to visit and identifies every web link in the page, adding these links to the list of URLs to visit. The process ends after one or more of the following conditions are met:

- Links have been followed to a specified depth.
- Maximum number of objects has been acquired.
- Maximum content size has been acquired.

By crawling a site at regular intervals using the time-to-live (or *ttl*) attribute, these links and their associated content can be updated regularly to keep the content fresh. Use the `<crawler>` tag to specify the website or FTP server crawler attributes. [Table B-1](#) lists the attributes, states whether these attributes are required or optional, and describes their functions.

Table B-1 Website or FTP Server Crawl Job Attributes

Attribute	Description
<i>start-url</i>	(Required) Identifies the URL to start the crawl job from. It can be a full path or a relative path. If it is a relative path, the <code><server></code> <code><host></code> tags are required to specify the origin server information.
<i>depth</i>	(Optional) Defines the level of depth to crawl the specified website. The depth is defined as the level of a website's URL links or FTP server's directory, where 0 is the URL or directory from which the crawl job starts. • 0—Acquire only the starting URL. • 1, 2, 3, and so on—Acquire the starting URL and its referred files to the depth specified. • -1 (not recommended)—Infinite or no depth restriction. Note It is not advisable to specify a depth of -1 because it takes a long time to crawl a large website and is wasteful if all the content on that particular website is not required. If the depth is not specified, the default is used. The default is 20.
<i>prefix</i>	(Optional) Combines the hostname from the <code><server></code> tag and this field to create a full prefix. Only content with URLs that match the full prefix are acquired, as shown in this example: <pre><server name="xx"> <host name="www.cisco.com" proto="https" port=433/> </server></pre> with the following <code><crawler></code> tag: <pre>prefix="marketing/eng/"</pre> The full prefix is "https://www.cisco.com:433/marketing/eng/." Only URLs that match this prefix are crawled. If a web page refers to ".../marketing/ops," the marketing/ops page and its children are not acquired. If the prefix is omitted, the crawler checks the default full prefix, which is the hostname portion of the URL from the server. In the example, the default full prefix is "https://www.cisco.com:433."

Table B-1 Website or FTP Server Crawl Job Attributes (continued)

Attribute	Description
<i>accept</i>	(Optional) Uses a regular expression to define acceptable URLs to crawl, in addition to having acceptable URLs match a prefix. For example, <i>accept</i> ="stock" means that only URLs that meet two conditions are crawled: the URL matches the prefix and also contains the regular expression string "stock."
<i>reject</i>	(Optional) Uses a regular expression to reject a URL if it matches the expression. The URL is first checked for a possible prefix match and then checked for a reject regular expression. If a URL does not match the prefix, it is immediately rejected. If a URL matches both the prefix and the reject regular expression, it is rejected by the expression.
<i>max-number</i>	(Optional) Specifies the maximum number of crawl job objects that can be acquired.
<i>maxTotalSizeInMB</i> <i>maxTotalSizeInKB</i> <i>maxTotalSizeInB</i>	(Optional) Specifies the maximum size of content that this crawl job can acquire. The size can be expressed in bytes (B), kilobytes (KB), or megabytes (MB). Note The maximum size of the file that is acquired is going to be less than the amount of disk space required to store the file. Files, when stored, contain overhead that contributes to the amount of disk space used for the delivery service. This overhead is approximately 20 KB per file. File size and storage overhead need to be taken into account when you are configuring the delivery service disk quota. This attribute replaces the <i>max-size-in-B/KB/MB</i> attribute. The <i>max-size-in-B/KB/MB</i> attribute continues to be supported for backward compatibility only.
<i>externalPrefixes</i>	(Optional) Specifies additional prefixes for crawl jobs to crawl multiple protocols or multiple websites. Prefixes are separated with a bar ().
<i>externalServers</i>	(Optional) Specifies additional hosts for crawl jobs. Can be used for multiple host crawl jobs where each host has a different user account. This attribute can be used to see the <host> tag with the proper authentication information.

**Note**

If you specify both the *max-number* and *maxTotalSizeIn* attributes as the criteria to use to stop a crawl job, the condition that is met first takes precedence. The crawl job stops either when the maximum number of objects is acquired or when the maximum content size is reached, whichever occurs first. For example, if the crawl job has acquired the maximum number of objects specified in the Manifest file but has not yet reached the maximum content size, the crawl job stops.

[Example B-2](#) shows a sample website crawl job.

Example B-2 Website Crawl Job

```
<server name="cisco">
  <host name="http://www.cisco.com/jobs/" />
</server>
<crawler
  server="cisco"
  start-url="eng/index.html"
  depth="10"
  prefix="eng/"
```

```

    reject=".pl"
    maxTotalSizeIn-MB="200"
  />

```

This website crawl job example contains the following attributes:

- The *start-url* path is `http://www.cisco.com/jobs/eng/index.html`.
- Search to a website link *depth* of 10.
- Search URLs with the *prefix* `http://www.cisco.com/jobs/eng/`
- Reject URLs containing `.pl` (Perl script pages).
- Only crawl until 200 megabytes in total content size are acquired.

If the server *name* attribute is omitted, the server *name* in the last specified `<server>` tag above it is used. If there are no `<server>` tags close by in the Manifest file, the server that hosts the Manifest file is used, which means that the relative URL is relative to the Manifest file URL.

Understanding the Prefix Attribute

When the *prefix* attribute is specified in the crawler tag, it refers to the prefix that must be added to the *start-url* when the Content Acquirer starts crawling a directory. This specifies the scope of the crawl, as shown in [Example B-3](#).

Example B-3 Scope of the Crawl

```

<CdnManifest>
<crawler start-url="http://172.19.227.33/"
        prefix="test/9"
        depth="2"
        />
</CdnManifest>

```

In this example, the crawl starts at:
`http://172.19.227.33/test/9`

When the *prefix* attribute is specified in the match tag, it specifies a filter that provides a short list of content that must be acquired, after a crawl job is started from a given *start-url*. When the Content Acquirer crawls, it could find several resources that need to be fetched. Each of the resources is identifiable using a URL. The *prefix* attribute in the match tag specifies the criteria to match before a URL is obtained. All URLs that match the given *prefix* are acquired.

In [Example B-4](#), only URLs that match “`http://linux-1.cisco.com/icons`” are acquired.

Example B-4 Crawl URL Matching

```

<CdnManifest>
<options timeZone="PDT" />
<crawler host="http://linux-1.cisco.com"
        start-url="test/MPEG_files"
        depth="1" >
<matchRule>
  <match prefix="http://linux-1.cisco.com/icons/" />
</matchRule>
</crawler>
</CdnManifest>

```

The *prefix* attribute in the crawler tag and the prefix in the match tag can coexist.

Writing Common Regular Expressions

A regular expression is a formula for matching strings that follow a recognizable pattern. The following special characters have special meanings in regular expressions:

. * \ ? [] ^ \$

If the regular expression string does not include any of these special characters, then only an exact match satisfies the search. For example, “stock” must match the exact substring “stock.”

Scheduling Content Acquisition

Two attributes, *ttl* and *prefetch*, are used to schedule content acquisition. Use *ttl* to specify the frequency of checking the content for freshness, in minutes. For example, to check for page freshness every day, enter `ttl="1440"`.

Example B-5 TTL Scheduling

In the following example, page freshness is scheduled to be checked once a day:

```
<item
  src="index.html"
  ttl="1440"
/>
```

In the following example, page freshness is scheduled to be crawled and checked every hour to a link *depth* value of 2:

```
<crawler
  start-url="index.html"
  depth="2"
  ttl="60"
/>
```

If the content is not yet available at a particular URL, the *prefetch* attribute can be used to specify the start time for acquisition at the specified URL. For example, `prefetch="2012-06-28 18:35:21"` means the content acquisition job can only start on June 28, 2012 and at the specified time.

The following example schedules a crawl of this website every hour to a link *depth* value of 2 to start on November 9, 2012 at 8:45 a.m.

```
<crawler
  start-url="index.html"
  depth="2"
  prefetch="2012-11-09 08:45:12"
  ttl="60"
/>
```

Specifying Shared Attributes

Attributes in single `<item>` tags can be shared or have the same attribute values. Instead of writing these attributes individually for every `<item>` tag, you can extract them and place them in a higher-level tag called `<item-group>`, where these attributes can be shared from this higher-level tag. You can create an `<item-group>` tag at a level below the `<CdnManifest>` tag, and write `<item>` tags into it as subtags, moving shared attributes into the `<item-group>` tag, as shown in [Example B-6](#).

Example B-6 Shared Attributes

```

<?xml version="1.0"?>
<CdnManifest>

<server name="cisco-cco">
  <host name="http://www.cisco.com"
    proto="http" />
</server>

<item-group
  server="cisco-cco"
  ttl="1440"
  type="prepos" >

  <item src="jobs/index.html"/>
  <item src="jobs/index1.html"/>
  <item src="jobs/index2.html"/>
  <item src="jobs/index3.html"/>
  <item src="jobs/index4.html"/>
  <item src="jobs/index5.html"/>

</item-group>

</CdnManifest>

```

You can also use the `<options>` tag to share attributes at the top-most level of the Manifest file. Shared attributes in the `<options>` tag can be shared by every `<item>` tag or by the `<crawler>` tag in the Manifest file. However, if a shared attribute is specified in both the `<item-group>` and the `<item>` tags or the `<options>` and `<item>` tags, attribute values in the `<item>` tags take precedence over the `<item-group>` and `<options>` tags.

The following example illustrates this precedence rule. The first `<item>` tag takes the `ttl` value 1440 from the `<options>` tag, but the second `<item>` uses its own `ttl` value of 60.

```

<options
  ttl="1440" >
<item src="index.html" />
<item src="index1.html" ttl="60" />

```

Specifying a Crawler Filter

With a rule-based crawler filter, you can crawl an entire website and only acquire contents with certain predefined characteristics. In contrast, crawler attributes in the `<crawler>` tag do not act as filters but only define the attributes for crawling. The `<matchRule>` tag is designed to act as a rule-based filter. You can define rule-based matches for file extensions, size, content type, and timestamp. [Example B-7](#), the crawl job is instructed to crawl the entire website starting at “index.html,” but to acquire only files with the .jpg extension and those larger than 50 kilobytes.

Example B-7 Crawler Filter

```

<crawler
  start-url="index.html" >
  <matchRule>
    <match minFileSizeIn-KB="50" extension="jpg" />
  </matchRule>
</crawler>

```

There can be multiple `<match>` subtags within a `<matchRule>` tag. Table B-2 describes the `<match>` subtag attributes.

Table B-2 *`<match>` Subtag Attributes*

Attribute	Description
<i>mime-type</i>	Specifies match of these MIME-types.
<i>extension</i>	Specifies match of files with these extensions.
<i>time-before</i>	Specifies match of files modified before this time (using the Greenwich mean time [GMT] time zone) in yyyy-mm-dd hh:mm:ss format.
<i>time-after</i>	Specifies match of files modified after this time (using the Greenwich mean time [GMT] time zone) in yyyy-mm-dd hh:mm:ss format.
<i>minFileSizeInMB</i> <i>minFileSizeInKB</i> <i>minFileSizeInB</i>	(Optional) Specifies match of content size equal to or larger than this value. The size can be expressed in megabytes (MB), kilobytes (KB), or bytes (B).
<i>maxFileSizeInMB</i> <i>maxFileSizeInKB</i> <i>maxFileSizeInB</i>	(Optional) Specifies match of content size equal to or smaller than this value. The size can be expressed in megabytes (MB), kilobytes (KB), or bytes (B).
<i>prefix</i>	(Optional) Specifies a prefix as a match rule to filter out websites during a crawl job.
<i>url-pattern</i>	(Optional) Specifies a regular expression as a match rule to filter out certain URLs.

A `<match>` subtag can specify multiple attributes. Attributes within a `<match>` tag have a Boolean AND relationship. In the following example, to satisfy this match rule, a file must have an .mpg type file extension and its size must be larger than 50 kilobytes.

```
<match extension="mpg" minFileSizeIn-KB="50" />
```

There is a Boolean OR relationship between the `<match>` rules themselves. A `<matchRule>` tag can have multiple `<match>` subtags, but only one of these subtags must be matched. The `<matchRule>` tag can be specified as a subtag of the `<crawler>` tag, or a subtag of the `<item-group>` tag. If there is a subtag in an `<item-group>` tag, it is shared by every `<crawler>` tag within that `<item-group>` tag.



Note

The *accept* or *reject* attributes can be mistakenly used in the `<crawler>` tag for a crawler filter.

For example, to crawl files with the extension .mpg, simply specifying `accept=".mpg"` is not correct. In this case, although specifying `accept=".mpg"` is not technically incorrect, no crawling occurs. Pages with URLs that do not match the *accept* constraint are not searched. For example, if the starting URL is index.html, this HTML file is parsed and any links not containing .mpg are rejected. If the .mpg files are located in the second or lower link levels, they are not fetched because the links connecting them have been rejected.

To properly crawl for the .mpg extension, use `<matchRule>`. Specify `<matchRule> <match extension=".mpg" />`. The whole site is crawled and only those files with the .mpg extension are retained.

The *url-pattern* attribute in the match tag specifies a filtering criteria for the crawl. As the Content Acquirer identifies resources that must be acquired, it validates the URL of those resources and content against the specified URL pattern and acquires them only if the pattern matches.

In the following example, the *url-pattern* value is a regular expression. The meaning of the regular expression is to not match URLs that have an mpeg extension. Only items that do not match the mpeg extension are acquired.

```
<CdnManifest>
<options timeZone="PDT" />
<crawler host="http://172.19.227.33"
        start-url="AD" >
<matchRule>
  <!-- exclude mpeg extension -->
  <match url-pattern=".[.](?!mpeg$).*$" />
</matchRule>
</crawler>
</CdnManifest>
```

Specifying Content Priority

A priority can be assigned to content objects to define their order of importance. The ECDS software determines the order of processing from the level of priority of the content. The higher the content priority, the sooner the acquisition of content from the origin server and the sooner the content is distributed to the Service Engines.



Note

Every content object acquired by running a crawl job has the same priority.

Three factors combine to determine content priority:

- Delivery Service priority—Content Distribution Priority drop-down list in the Acquisition and Distribution Properties area of the Delivery Service Definition page in the CDSM
- Item index—Content order listed in the Manifest file
- Item priority—Priority of the attributes specified in the `<item>` or `<crawler>` tag

To calculate content priority, use one of the following formulas:

- If there is a priority value for this content specified in the Manifest file *priority* attribute, use the following formula:

$$\text{Content priority} = \text{Delivery service priority} * 10000 + \text{Item priority}$$

In this formula, Item priority can be any integer and is unrestricted.



Tip

If you want a particular content object to have the highest priority, specify a very large integer value for item priority in the content priority formula.

- If an object does not have a priority value specified in the Manifest file *priority* attribute, use the following formula:

$$\text{Content priority} = \text{Delivery service priority} * 10000 + 10000 - \text{Item index}$$

In this formula, Item index is the order in which content is listed in the Manifest file.



Note

If there is no priority specified for any items, content is processed in the order listed in the Manifest file.

Generating a Playserver List

The ECDS software supports playservers that play back the following prefetched content types on the ECDS network: HTTP, HTTPS, RTSP, and RTMP (Movie Streamer, Windows Media, Flash Media Streaming).

The ECDS software checks whether the requested protocol matches the list in the playserver table. If it matches, the request is delivered. If it does not match, the request is rejected.

You can generate a playserver list in the following ways:

- By configuring playserver attributes in an `<item>` tag
- By configuring playserver MIME-type extension names in a `<playServerTable>` tag

To create the playserver list directly through the Manifest file, configure playserver attributes of the playserver list in an `<item>` tag. If an `<item>` tag does not have a playserver attribute, its playserver list is generated through the `<playServerTable>` tag. If the `<playServerTable>` tag is omitted in the Manifest file, a built-in default `<playServerTable>` tag is used to generate the playserver list. Multiple servers are separated by commas, as shown in the following example:

```
<item src="video.mpg" playServer="wmt,http" />
```

You can also generate the playserver list that supports these streaming media types through the `<playServerTable>` tag. The `<playServerTable>` tag maps content into a playserver list based on the MIME-type extension name. If there is a `<playServerTable>` tag in the Manifest file, use that tag.

To generate the playserver list through the `<playServerTable>` tag, use MIME-type extension names to configure which playserver can play the particular prefetched content, as shown in [Example B-8](#).

Example B-8 Playserver List

```
<playServerTable>
<playServer name="wmt">
  <extension name="wmv" />
  <extension name="wma" />
  <extension name="wmx" />
  <extension name="asf" />
</playServer>
<playServer name="http">
  <contentType name="application/pdf" />
  <contentType name="application/postscript" />
  <extension name="pdf" />
  <extension name="ps" />
</playServer>
</playServerTable>
```

The `<playServerTable>` tag is used to generate a playserver list for each content type. In the preceding example, any Portable Document Format (.pdf) or PostScript (.ps) file uses HTTP to play the content.

Customized Manifest Playserver Tables and the HTTP Playserver

In general, you do not need to specify your own playserver table or playserver in the Manifest file. A default playserver table maps appropriate file extensions or MIME-types to the proper playservers.

When you use the default playserver table, the HTTP playserver is always included in the playserver list, and this allows prefetched content to be played using HTTP. If the default playserver table does not meet your needs, you can customize your playserver lists by defining your own playserver table or by specifying a `playServer` attribute in the Manifest file.

The HTTP playserver is included in the default playserver table. However, if you specify your own playserver table or *playServer* attribute in the <item> or <crawler> tags, you must add the HTTP playserver to play HTTP content or other content using HTTP.

Specifying Attributes for Content Serving

Certain attributes in the Manifest file can be specified to control the manner in which content is served by the Service Engines. These attributes can be specified in the <item> and <crawler> tags. These same attributes can also be specified in the <item-group> or <options> tags, so they can be shared by their <item> and <crawler> subtags. [Table B-3](#) lists and describes these content-serving attributes.

Table B-3 **Attributes for Content Serving**

Attribute	Description
<i>serveStartTime</i>	(Optional) Designates a time in yyyy-mm-dd hh:mm:ss format at which the ECDS software is allowed to start serving the content. If the serving start time is omitted, content is ready to serve once it is distributed to the Service Engine.
<i>serveStopTime</i>	(Optional) Designates a time in yyyy-mm-dd hh:mm:ss format at which the ECDS software temporarily stops serving the content. If the serving stop time is omitted, the ECDS software serves the content to the Service Engine until the content is removed by modifying the Manifest file or renaming the delivery service.
<i>ignoreQueryString</i>	Playback attribute that can be used with the <options>, <item-group>, <item>, and <crawler> tags. If <i>ignoreQueryString</i> is set to true, then the ECDS software ignores any string after a question mark (?) in the request URL for playback. If this attribute is omitted, then the default value is false. For example, content with the request URL <code>url=http://web-server/foo</code> has been prefetched. If a user requests content with the URL <code>url=http://web-server/foo?id=xxx</code> and the <i>ignoreQueryString</i> attribute is set to false, then the ECDS software does not use prefetched content from the request URL <code>http://web-server/foo</code>. However, if the <i>ignoreQueryString</i> attribute is set to true, then the ECDS software treats the request URL <code>http://www-server/foo?id=xxx</code> the same as <code>http://www-server/foo</code> and returns prefetched content.
<i>wmtRequireAuth</i>	(Optional) Determines whether users need to be authenticated before the specified content is played. When <i>wmtRequireAuth</i> is set to true, the Service Engine requires authentication to play back the specified content to users and communicates with the origin server to check credentials. If the requests pass the credential check, the content is played back from the Service Engine. If this attribute is omitted, a heuristic approach is used to determine the setting: if the specified content is acquired by using a username and password, <i>wmtRequireAuth</i> is set to true; otherwise, it is set to false. For FTP, if the username is anonymous, <i>wmtRequireAuth</i> is set to false. Note If <i>wmtRequireAuth</i> is true, the Origin Server field in the CDSM Content Origin page for this delivery service needs to point to the server that can authenticate the users. When users want to play back the content, the server specified in the Origin Server field is checked for authentication.

Specifying Time Values in the Manifest File

The following attributes require that you enter a time value in the format yyyy-mm-dd hh:mm:ss (year-month-day hour:minute:second):

- *prefetch*
- *serveStartTime*
- *serveStopTime*
- *expires*
- *time-before*
- *time-after*

Manifest file time strings conform to the yyyy-mm-dd hh:mm:ss format. A time zone designation can be specified optionally at the end of a time string to indicate the particular time zone used. If a time zone designation is omitted, the GMT time zone is used. Note that automatic conversion between daylight saving time and standard time within a time zone is not supported, but a special designation for daylight saving time can be used, such as PDT for Pacific daylight saving time. In the following example, the prefetch time is September 5, 2012 at 09:09:09 Pacific daylight saving time:

```
<options timeZone="PDT" />
<item src="index.html" prefetch="2012-09-05 09:09:09 PDT" />
```

Refreshing and Removing Content

Use the *ttl* (time-to-live) and *expires* attributes of the Manifest file to monitor and control the freshness of content objects, and remove them.

The *ttl* attribute is expressed in minutes and specifies how frequently the software checks the freshness of the content at the origin server. If the *ttl* attribute is specified inside an `<item>` tag, it applies to that item; if it is specified inside a `<crawler>` tag, the attribute applies to the crawl job.

For example, if you give the *ttl* attribute a value of 10, the software checks the item or crawl job every 10 minutes. If the item has been updated, then the updated file is reacquired.



Caution

Sometimes a crawl job can be very large, crawling over thousands of files. The recrawl speed is 5000 files per hour for small files. It is time-consuming to recheck so many files. We strongly recommend that you specify a large *ttl* value for such crawl jobs (for example, 1440 minutes [daily]). Otherwise, the software continues to crawl the site over and over again, blocking other acquisition tasks.

If you omit the *ttl* attribute in the Manifest file, the time-to-live is assumed to be zero and the software does not recheck that item after it is acquired. A value of 0 (zero) for *ttl* means that the content is fetched only once and is never checked again unless you click the **Fetch Manifest Now** button in the CDSM or use the **acquirer start-delivery-service EXEC** command in the Content Acquirer CLI.

The **Fetch Manifest Now** button is located in the Delivery Service Content page in the CDSM. When you click this button, the software checks to see if the Manifest file has been updated, and the updated Manifest file is downloaded and reparsed. Also, regardless of whether the Manifest file has been updated, all content in the delivery service is rechecked and the updated content is downloaded.

If you assign a negative value to the *ttl* attribute, such as -1, that item is never to be rechecked. A negative *ttl* attribute value prevents the software from checking item freshness, even if you click the **Fetch Manifest Now** button or use the **acquirer start-delivery-service** command.

**Note**

Configuring the update interval in the CDSM GUI (**Services > Service Definition > Delivery Services > Delivery Service Content**) sets the interval for checking updates to the Manifest file itself. This setting only checks the Manifest file; it does not check the content.

The *failRetryInterval* attribute is sometimes confused with the *ttl* attribute. The fail and retry feature acts upon failed content or failed updates. If the acquisition of a single item or of some crawled content fails, the software automatically tries to refetch these failed objects after a default interval of 5 minutes. The fail and retry interval can also be specified by using the *failRetryInterval* attribute in the Manifest file.

The difference between the *failRetryInterval* attribute and the *ttl* attribute is that the *ttl* attribute is for successfully acquired content and the *failRetryInterval* attribute is for content acquisition failures. The *ttl* attribute must be specified for the software to recheck the content freshness, whereas the *failRetryInterval* attribute does not need to be specified unless you want to change the retry interval.

The *expires* attribute specifies the time the content is to be removed from the ECDS network. If you do not specify a time when you set the *expires* attribute, content is stored in the ECDS network until it is explicitly removed when you modify the Manifest file. The *expires* attribute uses the format yyyy-mm-dd hh:mm:ss (year-month-day hour:minute:second). In the following example, the content expires on June 12, 2012 at 2:00 p.m.

```
expires="2012-06-12 14:00:00 PST"
```

If the *expires* attribute is specified inside an <item> tag, it applies to that item; if it is specified inside a <crawler> tag, the attribute applies to the crawl job.

You can monitor the status of content replication and freshness by enabling and then viewing the transaction log files that reside on the Service Engines. To verify whether or not a content object or file was successfully imported to or refreshed on a particular Service Engine, take these actions:

- Enable the transaction log function on the Service Engine you want to monitor.
- View the transaction log entries for the content object or filename that resides on that Service Engine.

Specifying Live Content

Only Windows Media live contents can be specified in the Manifest file. Use the <item> tag and specify the *type* attribute as wmt-live, as shown in [Example B-9](#). The live stream for the wmt-live content type is url=rtsp://www.company-web-site.org/tmp/ceo-talk.

Example B-9 Windows Media Live Content

```
<CdnManifest>
<server name="wmt-server">
<host name="rtsp://www.company-web-site.org" />
</server>
<item src="/tmp/ceo-talk" type="wmt-live" >
</item>
<!--
This is a "wmt-live" streaming content type specified by the "type" attribute. The live
stream URL is
rtsp://www.company-web-site.org/tmp/ceo-talk.
-->
</CdnManifest>
```


**Note**

If you are using the Manifest file for live streaming, the origin server configured for the delivery service should be the same as the encoder IP address.

Specifying Hybrid Ingest Content

For hybrid ingested content, the content is not prefetched into the ECDS network. Instead, the content is ingested dynamically based on the user request. This type of ingest is called *dynamic ingest* or *on-demand ingest*. To control the play back of the on-demand content, a new type of ingest has been introduced called *hybrid ingest*. In this method, the metadata for on-demand contents can be specified in the Manifest file. However, the actual content is not acquired by the Content Acquirer.

Hybrid ingest is supported by specifying “cache” as the value for the *type* attribute inside the <item> tag.

**Note**

This mode of ingest is supported only for single items; crawling is not supported.

[Example B-10](#) shows the Manifest file for hybrid ingest content.

Example B-10 Hybrid Ingest Content

```
<CdnManifest>
<server name="web-server">
<host name="http://www.company-web-site.org" />
</server>
<item src="/tmp/ceo-talk.wmv" type="cache"
      serveStartTime="2012-01-12 14:00:00 PST"
      serveStopTime="2012-04-12 14:00:00 PST"
>
</item>
</CdnManifest>
```

**Note**

For type= “cache,” <host> and <server> tags are not used.

**Note**

Currently, only *serveStartTime* and *serveStopTime* are supported for type= “cache.”

Manifest Validator Utility

Because correct Manifest file syntax is so important to the proper deployment of prefetched content on your ECDS network, Cisco makes available a Manifest file syntax validator. The Manifest Validator, a Java-based command-line interface that verifies the correctness of the syntax of the Manifest file you have written or modified, is built into the CDSM.

The Manifest Validator utility tests each line of the Manifest file to identify syntax errors where they exist and determine whether or not the Manifest file is valid and ready for use in importing content into your ECDS network.

See the following sections for more information:

- [Running the Manifest Validator Utility, page B-16](#)

- [Understanding Manifest File Validator Output, page B-18](#)
- [Correcting Manifest File Syntax, page B-19](#)

Running the Manifest Validator Utility



Note

You must first create a new delivery service or edit an existing delivery service before you can access the Manifest Validator. See the [“Configuring Delivery Services” section on page 8-1 of Chapter 8, “Configuring Services.”](#)

To access the Manifest Validator:

Step 1 Choose **Services > Service Definition > Delivery Services > Tools > Manifest Validator**.

Step 2 In the **Manifest File** field, enter the URL of the Manifest file you want to test.

Step 3 Click **Validate**.

The Manifest Validator checks the syntax of your Manifest file to make sure that source files are named for each content item in the Manifest file. It then checks the URL for each content item to verify that the content is placed correctly and then displays the output in the lower part of the page. The Manifest Validator does not determine the size of the item.

Alternatively, click **Validate** in the Delivery Service Content page. The results are displayed in a new window.

See the following:

- [Valid Manifest File Example](#)
- [Invalid Manifest File Example](#)

Valid Manifest File Example

The following is an example of a valid Manifest file:

```
<CdnManifest>
<item
    src="tmp/mao's.html"
    priority="20"
/>
<server name="my-dev'box">
<host name="http://128.107.150.26"
    proto="http" />
</server>

<item
    src="tmp/lu.html"
    priority="300"
/>
<item
    src="/tmp/first_grader.html"
/>
<server name="server0">
    <host name="http://umark-u5.cisco.com:8080/" />
</server>
```

```

<item  •src="a.gif"/>
<server name="server1">
    <host name="http://unicorn-web" />
</server>
<item  •src="Media/wmtfiles/DCA%20Disk%201/Microsoft_Logos/Logos_100k.wmv" />

</CdnManifest>

```

The final lines of the Manifest Validator output indicate whether the Manifest file is valid or not. Wait until the following message is displayed, indicating that the validator has completed processing the Manifest file:

```

Total Number of Error: 0
Total Number of Warning: 0
Manifest File is CORRECT.

```

If errors are found, the error messages appear before the preceding message.

Invalid Manifest File Example

The following text is an example of an invalid Manifest file:

```

<CdnManifest>
<item
    src="tmp/mao's.html"
    priority="20"
/>
<server name="my-dev'box">
<host name="http://128.107.150.26"
    proto="http" />
</server>
<item
    src="tmp/lu.html"
    priority="300"
/>
<item
    src="/tmp/first_grader.html"
/>
<server name="server0">
    <host name="http://umark-u5.cisco.com:8080/" >
</server>
<item src="a.gif"/>
<server name="server1">
    <host name="http://unicorn-web" />
</server>
<item src1="Media/wmtfiles/DCA%20Disk%201/Microsoft_Logos/Logos_100k.wmv" />
</CdnManifest>

```

In the preceding example, although there are no warnings, two errors are found, and this Manifest file is syntactically incorrect, as shown in the following message:

```

ERROR (/state/dump/tmp.xml.1040667979990 line: 23 col: 1 ):No character data is allowed by
content model
ERROR (/state/dump/tmp.xml.1040667979990 line: 23 col: 9 ):Expected end of tag 'host'
Manifest File: /state/dump/tmp.xml.1040667979990
Total Number of Error: 2
Total Number of Warning: 0
Manifest File is NOT CORRECT!

```

The following full-text output is an example of the invalid Manifest file after the Manifest Validator checks the file:

```

Manifest validated: http://qiwzhang-lnx/nfs-obsidian/Unicorn/my-single-bad.xml

```

```

The manifest is downloaded as /state/dump/tmp.xml.1040667979990 for validation, this file
will be removed when validation is completed.
Start CdnManifest
Start item
    priority=20
    src=tmp/mao's.html
End item

Start server
    name=my-dev'box
Start host
    name=http://128.107.150.26
    proto=http
    uuencoded=false
End host

End server

Start item
    priority=300
    src=tmp/lu.html
End item

Start item
    src=/tmp/first_grader.html
End item

Start server
    name=server0
Start host
    name=http://umark-u5.cisco.com:8080/
    uuencoded=false
ERROR (/state/dump/tmp.xml.1040667979990 line: 23 col: 1 ):No character data is allowed by
content model
ERROR (/state/dump/tmp.xml.1040667979990 line: 23 col: 9 ):Expected end of tag 'host'
Manifest File: /state/dump/tmp.xml.1040667979990
Total Number of Error: 2
Total Number of Warning: 0
Manifest File is NOT CORRECT!

```

Understanding Manifest File Validator Output

The Manifest Validator messages appear below the Manifest File in the Manifest Validator page.

Each output file has a similar structure and syntax. It clearly identifies any errors or warning messages arising from incorrect Manifest file syntax. Manifest files are determined by the validator to be either:

- **CORRECT**—Contains possible syntax irregularities but is syntactically valid and ready for deployment on your ECDS network
- **INCORRECT**—Contains syntax errors and is unsuitable for deployment on your ECDS network

See the following sections for more information:

- [Syntax Errors, page B-19](#)
- [Syntax Warnings, page B-19](#)

Syntax Errors

The Manifest Validator issues syntax errors only when it cannot identify a source file for a listed content item, either because it is not listed or because it is listed using improper syntax. Files containing syntax errors are marked INCORRECT.

Syntax errors are identified in the output with the ERROR label. In addition to the label, the line and column number containing the error are provided, as well as the Manifest file attribute for which the error was issued. An error appears in the following example:

```
ERROR (/state/dump/tmp.xml.1040667979990 line: 23 col: 1 ):No character data is allowed by
content model
```

In the error example:

- `/state/dump/tmp.xml.1040667979990` is the Manifest file name
- `line: 23 col: 1` is the Manifest file line and column number where the error occurs
- `No character data is allowed by content model` describes the type of Manifest file error

Syntax Warnings

The Manifest Validator issues syntax warnings for a wide variety of irregularities in the Manifest file syntax. Files containing syntax warnings may be marked CORRECT or INCORRECT, depending on whether or not syntax errors have also been issued.

Syntax warnings are identified in the output with the WARNING label. In addition to this warning label, the line number for which the warning is issued is provided, as well as the Manifest file attribute, valid options, and the default value for that attribute for which the warning was issued.

Correcting Manifest File Syntax

Once you have identified syntax warnings, errors, and messages using the output from the Manifest Validator, you can correct your Manifest file syntax and then rerun the Manifest Validator on the corrected file to verify its correctness.

It is a good idea to review every warning and error in your Manifest file. Some warnings, although they still allow the Manifest Validator to find your Manifest file syntax to be correct, can be the source of problems when you deploy the identified content to your ECDS network.

Manifest File Structure and Syntax

The ECDS Manifest file provides powerful features for representing and manipulating ECDS network data that can be easily edited using any simple text editor. See the following sections for more information:

- [Manifest File Tag Summary, page B-20](#)
- [Manifest File Nested Tag Relationships, page B-22](#)
- [Manifest File Tag Descriptions, page B-23](#)

Manifest File Tag Summary

Table B-4 provides a summary list of the Manifest file tags, their corresponding attributes and subelements, and a brief description of each tag. Table B-5 shows an example of how tags are nested in a Manifest file. The sections that follow provide a more detailed description of the Manifest file tags, the data they contain, and their attributes.

Table B-4 Manifest File Tag Summary

Tag Name	Subelements	Attributes		Description
CdnManifest	<playServerTable/> <options/> <server/> <item/> <item-group/> <crawler/>	None		Marks the beginning and end of the Manifest file content.
playServerTable	<playServer/>	None		(Optional) Sets default mappings for media types.
playServer	<contentType/> <extension/>	name Note Attributes that are required for a tag are shown in boldface italic font.		Names the media server type on the Service Engine responsible for playing content types and files with extensions mapped to it using <contentType> tags.
contentType	None	name		(Optional, but must have either <contentType> or <extension> tag.) Names the MIME-type content mapped to a playserver.
extension	None	name		(Optional, but must have either <contentType> or <extension> tag.) Names the file extension that is mapped to a playserver.
options	<schedule/> <repeat/>	<i>enableCookies</i> <i>expires</i> <i>failRetryInterval</i> <i>ignoreOriginPort</i> <i>ignoreQueryString</i>	<i>prefetch</i> <i>priority</i> <i>wmtRequireAuth</i> <i>server</i> <i>sslAuthType</i> <i>timeZone</i> <i>ttl</i> <i>type</i>	(Optional) Defines attributes specific to the Manifest file that can be shared.
server	<host/>	name		Defines <i>only</i> one host from which content is to be retrieved.
host	None	name <i>disableBasicAuth</i> <i>noProxy</i> <i>ntlmUserDomain</i> <i>password</i> <i>port</i> <i>proto</i>	<i>proxyServer</i> <i>sslAuthType</i> <i>user</i> <i>userDomainName</i> <i>uuencoded</i>	Defines a web server or live server from which content is to be retrieved and later prefetched. The hostname can be specified as: proto://user:password@hostname:port

Table B-4 Manifest File Tag Summary (continued)

Tag Name	Subelements	Attributes	Description
proxyServer	None	serverName <i>disableBasicAuth</i> <i>ntlmUserDomain</i> <i>password</i> <i>port</i> <i>user</i> <i>uuencoded</i>	Specifies proxy server information.
item	<contains/> <schedule/> <repeat/>	src <i>authCookie</i> <i>cdn-url</i> <i>disableBasicAuth</i> <i>enableCookies</i> <i>expires</i> <i>failRetryInterval</i> <i>host</i> <i>ignoreOriginPort</i> <i>ignoreQueryString</i> <i>noProxy</i> <i>ntlmUserDomain</i> <i>password</i> <i>playServer</i> <i>port</i> <i>prefetch</i> <i>priority</i> <i>proto</i> <i>proxyServer</i> <i>server</i> <i>serveStartTime</i> <i>serveStopTime</i> <i>sslAuthType</i> <i>ttl</i> <i>type</i> <i>user</i> <i>userDomainName</i> <i>uuencoded</i> <i>wmtRequireAuth</i>	Identifies specific content that is to be acquired from the origin server.
crawler	<matchRule/> <schedule><repeat>	start-url <i>accept</i> <i>authCookie</i> <i>cdnPrefix</i> <i>depth</i> <i>disableBasicAuth</i> <i>enableCookies</i> <i>expires</i> <i>externalPrefixes</i> <i>externalServers</i> <i>failRetryInterval</i> <i>host</i> <i>ignoreOriginPort</i> <i>ignoreQueryString</i> <i>keepExpiredContent</i> <i>keepFolder</i> <i>keepNoCacheContent</i> <i>keepQueryUrl</i> <i>max-number</i> <i>maxTotalSizeIn-MB</i> <i>noProxy</i> <i>ntlmUserDomain</i> <i>password</i> <i>playServer</i> <i>port</i> <i>prefetch</i> <i>prefix</i> <i>priority</i> <i>proto</i> <i>proxyServer</i> <i>reject</i> <i>reportBrokenLinks</i> <i>serveStartTime</i> <i>serveStopTime</i> <i>server</i> <i>srcPrefix</i> <i>sslAuthType</i> <i>ttl</i> <i>type</i> <i>user</i> <i>userDomainName</i> <i>uuencoded</i> <i>wmRequireAuth</i>	Supports crawling of a website or FTP server.

Table B-4 Manifest File Tag Summary (continued)

Tag Name	Subelements	Attributes		Description
item-group	<item/> <crawler/> <item-group/>	<i>cdnPrefix</i> <i>cdn-url</i> <i>disableBasicAuth</i> <i>enableCookies</i> <i>expires</i> <i>failRetryInterval</i> <i>host</i> <i>ignoreOriginPort</i> <i>ignoreQueryString</i> <i>noProxy</i> <i>password</i> <i>playServer</i> <i>prefetch</i> <i>priority</i>	<i>proto</i> <i>proxyServer</i> <i>requireAuth</i> <i>serveStartTime</i> <i>serveStopTime</i> <i>server</i> <i>srcPrefix</i> <i>sslAuthType</i> <i>ttl</i> <i>type</i> <i>user</i> <i>userDomainName</i> <i>uuencoded</i> <i>wmtRequireAuth</i>	Places shared attributes under one tag so that they can be shared by every <item> and <crawler> tag within that group.
matchRule	<match>	None	—	(Optional) Defines additional filter rules for crawler jobs.
match	None	<i>extension</i> <i>mime-type</i> <i>prefix</i> <i>minFileSizeIn-B</i> <i>minFileSizeIn-KB</i> <i>minFileSizeIn-MB</i>	<i>maxFileSizeIn-B</i> <i>maxFileSizeIn-KB</i> <i>maxFileSizeIn-MB</i> <i>time-after</i> <i>time-before</i> <i>url-pattern</i>	(Optional) Specifies the acquisition criteria of content objects before they can be acquired by the ECDS network.
contains	None	<i>cdn-url</i>	—	(Optional) Identifies content objects that are embedded within the content item currently being described.

Manifest File Nested Tag Relationships

[Table B-5](#) lists nested tag relationships.

Table B-5 Manifest File Nested Tag Relationships

<CdnManifest>				
	<playServerTable> <playServer>			
		<contentType /> <extension />		
			</playServerTable> </playServer>	
	<options>			
		Manifest file shared attributes	</options>	

Table B-5 *Manifest File Nested Tag Relationships (continued)*

	<server>			
		<host/>		
			</server>	
	<item>			
		<contains />		
			</item>	
	<crawler>			
		<matchRule/>		
			</crawler>	
	<item-group>			
		<contains />		
			</item-group>	
				</CdnManifest>

Manifest File Tag Descriptions

- [CdnManifest](#)
- [playServerTable](#)
- [playServer](#)
- [contentType](#)
- [extension](#)
- [options](#)
- [server](#)
- [host](#)
- [proxyServer](#)
- [item](#)
- [crawler](#)
- [item-group](#)
- [matchRule](#)
- [match](#)
- [contains](#)

CdnManifest

The<CdnManifest> </CdnManifest> tag set is required and marks the beginning and end of the Manifest file content. At a minimum, each <CdnManifest> tag set must contain at least one item, or content object, that is fetched and stored.

Attributes

None

Subelements

The <CdnManifest> tag set can contain the following subelements:

- playServerTable
The <CdnManifest> tag set can contain only one playServerTable subelement.
- options
The <CdnManifest> tag set can contain only one options subelement.
- server
- item
- item-group
- crawler

Example

```
<CdnManifest>
  <server name="origin-server">
    <host name="www.name.com" proto="http" port="80" />
  </server>
  <item cdn-url= "logo.jpg" server="originserver" src= "images/img.jpg" type="prepos"
    playServer="http" ttl="300" />
</CdnManifest>
```

playServerTable

The <playServerTable> </playServerTable> tag set is optional and provides a means for you to set default mappings for a variety of media types. Mappings can be set for both MIME-type content (the preferred mapping) and file extensions. Playserver tables allow you to override default mappings on the Service Engine for content types from a particular origin server. Playservers can be any one of the following streaming servers: WMT, HTTP, QTSS, or FMS. If no <playServerTable> tag is configured in the Manifest file, a default <playServerTable> tag is used.

Using the Manifest file, you can map groups of single items as well as individual content objects to an installed playserver. The following are content item and Manifest file playserver mappings:

- Content item URL
Playserver mappings appear immediately after the origin server name in place of the default <CdnManifest> tag.
- Manifest file as an attribute of the <item> or <item-group> tag
Playserver mappings placed at this location are identified using the *playServer* attribute and only apply to the named item or group of items.
- Manifest file as a playserver table
Mappings are grouped within the <playServerTable> and <playServer> tags and are applied to content served from the origin server as directed by the Manifest file.
- System-level
Playserver mappings are configured during ECDS software startup.

The <playServerTable> tags are enclosed within the <CdnManifest> tags and name at least one of four playservers, such as RealServer, to which certain MIME-types and file extensions are mapped.

Attributes

None

Subelements

The <playServerTable> element must contain at least one <playServer> tag.

playServer

The <playServer> </playServer> tag set is required for the <playServerTable> tag and names the media server type on the Service Engine that is responsible for playing the content types and files with extensions mapped to it using the <contentType> tags. The <playServer> tag is enclosed within <playServerTable> tags.

**Note**

Do not confuse the <playServer> tag with the *playserver* attribute in an <item> or <item-group> tag. An <item> or <item-group> tag specifies a server type to be used for an individual content object or group of related content objects. Although both playserver settings accomplish the same task, <item> tag-level playserver settings take precedence over the content type and file extension mappings specified by the <playServer> tags in the <playServerTable> tag.

Attributes

The <playServer> tag name is required. Each <playServer> tag names the type of server to which content is mapped using the *name* attribute. The Service Engines support the following types of playservers:

- http: HTTP web server
- qtss: Apple QuickTime Streaming Server
- wmt: Microsoft Windows Media Technologies
- fms: Flash Media Streaming Server

Subelements

At least one of the following subelements must be present in a <playServer> tag set.

- <contentType />
- <extension />

contentType

The <contentType /> tag is optional but either a <contentType /> or an <extension /> subelement must be present in a <playServer> tag set. The <contentType /> tag names MIME-type content that is to be mapped to a playserver. The <contentType /> tag must be enclosed within a <playServer> tag set. When both <contentType /> and <extension /> tags are present in a <PlayServerTable> tag for a particular media type, the <contentType /> mapping takes precedence.

Attributes

Each <contentType /> tag names a media content type that is to be mapped to the playserver using the *name* attribute. The *name* attribute is required.

Subelements

None

extension

The `<extension />` tag is optional but either a `<contentType />` or an `<extension />` subelement must be present in a `<playServer>` tag set. The `<extension />` tag names the file extension that is being mapped to a playserver.

The `<extension />` tag follows the `<playServer>` tag. When both `<contentType />` and `<extension />` tags are present in the `<playServer>` tag for a particular media type, the `<contentType />` mapping takes precedence.

Attributes

The *name* attribute is required and provides the file extension for a mapped content type. When files with the named extension are requested, the mapped playserver is used to serve them.

Subelements

None

Example

```
<CdnManifest>
<playServerTable>
<playServer name="wmt">
    <extension name="asf" />
</playServer>
<playServer name="http">
    <contentType name="application/pdf" />
    <contentType name="application/postscript" />
    <extension name="pdf" />
    <extension name="ps" />
</playServer>
</playServerTable>
<server name="test.origin.com/">
    <host name="http://tst.orgn.com" proto="http" />
</server>
<item
    src="pic1.mpg"
/>
</CdnManifest>
```

options

The `<options/>` tag is optional and used to define attributes specific to the Manifest file. Shared attributes can be inherited by `<item>` and `<crawler>` tags in the Manifest file. For example, *timeZone* is an attribute specific to the Manifest file that is used to set the time zone for all time-related values. Attributes such as *ttl* can exist as `<options/>` tags, and their values can be shared by all `<item>` and `<crawler>` tags within the Manifest file.

The `<options/>` tag set is enclosed within the `<CdnManifest>` tag set and specifies at least one global setting. No more than one `<options>` tag is allowed per Manifest file.

If parameters are defined within the Manifest file `<options/>`, `<item-group>`, or `<item>` tags, the order of precedence from lowest to highest is `<options/>`, `<item-group>`, and `<item>`.

Attributes

The *timeZone* attribute specifies the time zone for time values of attributes such as *expires* and *prefetch*.

The following list of attributes can be shared by `<item>` and `<crawler>` tags. See the [“item” section on page B-30](#) for descriptions of the following attributes:

- *enableCookies*
- *expires*
- *failRetryInterval*
- *ignoreOriginPort*
- *ignoreQueryString*
- *prefetch*
- *priority*
- *wmtRequireAuth*
- *server*
- *sslAuthType*
- *ttl*
- *type*

Subelements

<schedule><repeat>

(See the [“item” section on page B-30](#) for descriptions of these subelements.)

server

The <server> and <host> tag fields configure the origin content source server. The <host> tag field inside the <server> tag field configures the content source host. Having multiple <host> tag fields in one <server> tag field is not supported.

Each <item> or <item-group> tag can have a *server* attribute that refers to this <server> tag field. The <server> </server> tag set is required and defines only one host from which content is to be retrieved. The <server> tags are contained within <CdnManifest> tags and contain one <host> tag that identifies the host from which content is retrieved.

Attributes

The *name* attribute is required and can be any name as long as it matches the *server* attribute values in the <item> or <crawler> tags.

Subelements

The <server> tag set can only contain one <host/> subelement.

host

The <host/> tag is required and defines a web server or live server from which content is to be retrieved and later prefetched. Only one host can be defined within a single <server> tag set. The <host/> tag must be enclosed within <server> tags.

Attributes

- *disableBasicAuth*

The *disableBasicAuth* attribute is optional; if specified, basic authentication is disabled.

- *name*

The *name* attribute is required and identifies the domain name or IP address of the host, unless the *proto* attribute field is empty. If the *proto* attribute field is empty, the *name* attribute must be a fully qualified URL, including scheme and domain name or IP address. It can also include subdirectories, such as `http://www.abc.com/media`.

The *name* attribute can also contain the UNC path to an SMB server; for example, `\\SMBserver\directory\`.

- *noProxy*

The *noProxy* attribute is optional. If set to true, no proxy is used for the origin server. The default is false.

- *ntlmUserDomain*

The *ntlmUserDomain* attribute is optional and specifies the user domain name for NTLM authentication.

- *password*

The *password* attribute is optional and identifies the password for the user account that is required to access the host server.

- *port*

The *port* attribute is optional and identifies the TCP port through which traffic to and from the host passes. The port used depends on the protocol used. The default port for HTTP is 80. The *port* attribute is only required for a nonstandard port assignment. The port attribute can also be specified in the *name* attribute, such as `name="http://www.cisco.com:8080/."`

- *proto*

The *proto* attribute is optional and identifies the communication protocol that is used to fetch content from the host. Supported protocols are HTTP, HTTPS, MMS-over-HTTP, or FTP. The default *proto* attribute is HTTP. The *proto* attribute can be empty if the *name* attribute is a fully qualified domain name (FQDN).

- *proxyServer*

The *proxyServer* attribute is optional and specifies which proxy server to use if there are multiple `<proxyServer>` tags in the Manifest file. If no proxy server is specified, the server in the closest `<proxyServer>` tag is used.

- *sslAuthType*

The *sslAuthType* attribute is optional and has two possible values for the type of SSL certificate verification:

- *strong*—Strong authentication. If any errors occur during certificate verification by the acquirer module, content from that site is not acquired. The default *sslAuthType* attribute setting is strong.
- *weak*—Weak authentication. If certain errors occur during certificate verification by the acquirer module, content from that site continues to be acquired. These errors are as follows:

Unable to decode issuer's public key

Certificate has expired

Self-signed certificate

Self-signed certificate in certificate chain

Unable to get local issuer certificate

Subject issuer mismatch

Authority and issuer serial number mismatch

The Content Acquirer is not marked as trusted

Unable to verify the first certificate

Certificate is not yet valid

Certificate has invalid purpose

- *user*

The *user* attribute is optional and identifies the secure login used for host access.

- *userDomainName*

See the “[item](#)” section on page B-30 for a description of this attribute.

- *uuencoded*

The *uuencoded* attribute is optional. If set to true, the password is not encoded. The *uuencoded* attribute default setting is false.

Subelements

None

proxyServer

The <proxyServer> tag specifies proxy server information. The <proxyServer> tag must be located at the top level of the Manifest file, directly under the <CdnManifest> tag; it cannot be used as a subtag of any other tags, as shown in this example:

```
<CdnManifest>
<proxyServer>
...
</CdnManifest>
</proxyServer>
```

Attributes

- *disableBasicAuth*

The *disableBasicAuth* attribute is optional; if specified, basic authentication is disabled.

- *ntlmUserDomain*

The *ntlmUserDomain* attribute is optional and specifies the user domain name for NTLM authentication.

- *password*

The *password* attribute is optional and identifies the password for the user account that is required to access the proxy server.

- *port*

The *port* attribute is optional and specifies the proxy port.

- *serverName*

The *serverName* attribute is required and identifies the domain name or IP address of the proxy server.

- *user*

The *user* attribute is optional and identifies the secure login used for proxy authentication.

- *uuencoded*

The *uuencoded* attribute is optional and designates whether the password is to be encoded.

Subelements

None

item

The `<item> </item>` tag set identifies the specific content that is to be acquired. The `<item>` tag names a single piece of content or a content object on the origin server, such as a graphic, MPEG video, or RealAudio sound file. Content items can be listed individually or grouped using the `<item-group>` tag.

The `<item>` tag must be enclosed within the `<CdnManifest>` tag set and can also be enclosed within `<item-group>` tags.

Attributes

- *src*

The *src* attribute is required and identifies the URL from which to fetch the content. The URL can be a full URL or a relative URL. A full URL has the following format:

`proto://username:password@/domain-name:port/file-path/file-name`

Protocols supported in the *src* attribute are HTTP, HTTPS, FTP, and SMB. For SMB, the URL must be written in UNC format (`\\SMBserver\directory\file`).

If a relative path is used, the `<server>` and `<host>` tags are required to specify origin server information, as shown in this example:

```
<item src="http://user:password@www.cisco.com/HR/index.html" />
<server name="ftp-server" >
  <host name="ftp://ftp-server" user="johw" password="www" />
</host>
<item src="data/video.asf" />
```



Note

A URL containing a question mark (?) is not supported. A Manifest file parsing error occurs if you specify a URL that contains a question mark.



Note

A URL containing a pound sign (#) is modified. All characters that follow a pound sign are discarded, including the pound sign itself.

- *host*

The *host* attribute specifies the hostname if the source URL of the *src* attribute is a relative URL.

- *server*

The *server* attribute is optional and refers to the server name in the `<server>` tag. If the *server* attribute is omitted, the server listed in the closest `<server>` tag is used. If there is no `<server>` tag close to this item, the Manifest file server is used.

- *cdn-url*

The *cdn-url* attribute is optional and is used when content needs to be acquired from one URL (the content acquisition URL) and published using another URL (the publishing URL). The *cdn-url* attribute is the relative ECDS network URL that end users use to access this content. If no *cdn-url* attribute is specified, then the *src* attribute is used as the relative ECDS network URL.

In the following sample Manifest file, the content item being acquired contains the file path /RemAdmin/InternalReview/firstpage.htm. By specifying a new file path (RemAdmin/Production/firstpage.htm) using the *cdn-url* attribute, the publishing URL disguises the fact that the content originated from an “Internal Review.”

```
<CdnManifest>
<server name="ultra-server">
  <host name="http://ultra-server" />
</server>
<item src="RemAdmin/InternalReview/firstpage.htm"
cdn-url="RemAdmin/Production/firstpage.htm" />
</CdnManifest>
```

In the preceding example, *src* is the content acquisition URL and *cdn-url* is the publishing URL.



Note The content item file path (RemAdmin/InternalReview/firstpage.htm) is controlled by the Manifest file. The *cdn-url* attribute associates a file path with the content item in the Manifest file. The Manifest file allows the file path for the *cdn-url* attribute to be specified independently of the file path from which the content items are to be acquired from the origin server (*src* attribute), allowing the publishing URL to differ from the content acquisition URL.

If the content requires playback authentication or is live content, the origin server from which the content is acquired has to be contacted. Therefore, two URLs must exist for the same content item, and the URL specified in the *cdn-url* attribute must exist on the origin server at all times.

For example, if the content item “RemAdmin/Production/firstpage.htm” in the preceding example requires playback authentication, this content must exist on the “ultra-server” origin server. Otherwise, prefetched content playback fails.

In general, you should not use the *cdn-url*, *cdnPrefix*, or *srcPrefix* attributes if playback authentication is required or if the content is live.

If you use FTP to acquire content and the content type is not specified in the Manifest file and the *cdn-url* attribute is specified to alter your publishing URL, the *cdn-url* attribute must have the correct file path extension. Otherwise, the incorrect content type is generated and you cannot play the content.

The following example correctly shows the publishing URL with the same file path extension (.jpg) as the origin server URL.

```
<item src="ftp://ftp-server.abc.com/pictures/pic.jpg" cdn-url="pic.jpg" />
```

The following example is incorrectly written, because it does not specify the file path extension (.jpg) in the *cdn-url* attribute.

```
<item src="ftp://ftp-server.abc.com/pictures/pic.jpg" cdn-url="pic" />
```

- *type*

The *type* attribute is optional and defines whether content is to be prefetched or live on the ECDS network. The three *type* attributes are *prepos*, *cache*, and *wmt-live*. The *wmt-live* type attribute is used to deliver live content. The *cache* type corresponds to hybrid ingest method. If this field is left blank, the default type is *prepos*.



Note For type="cache", <host> and <server> tags are not used.



Note Currently, only *serveStartTime* and *serveStopTime* are supported for the type="cache" attribute.

- *playServer*

The *playServer* attribute is optional and names the server used to play back the content. Valid play servers are wmt (Windows Media Technologies), qtss (QuickTime Streaming Server), fms (Flash Media Streaming), and http (Web Engine). The value in this field is either one play server or multiple play servers separated by commas. If a value for this attribute is not specified, the <PlayServerTable> tag in the Manifest file is used to generate the play server list for this content. If the Manifest file does not have the <PlayServerTable> tag specified, it uses the default <PlayServerTable> tag.

- *prefetch*

The *prefetch* attribute is optional and specifies a time (in yyyy-mm-dd hh:mm:ss [year-month-day hour:minute:second] format) for the first content acquisition or re-check after the Manifest file is parsed. The time zone for the time can be specified in the <options> tag. Note that the autoconversion between daylight saving time and standard time within a time zone is not supported, but a special designation for daylight saving time can be used, such as PDT for Pacific daylight saving time. In the following example, the prefetch time is September 5, 2012 at 09:09:09 Pacific daylight saving time.

```
<options timeZone="PDT" />
<item src="index.html" prefetch="2012-09-05 09:09:09 PDT" />
```

This attribute is used when you want to specify a future time for the acquirer to begin fetching content from the origin server. When a future time is specified, the acquirer does not acquire content before this time; however, it checks content freshness during its scheduled *ttl* interval. If a *prefetch* time is omitted, the content is acquired immediately.

After the Manifest file is parsed, if any items or crawl tasks have changed or new ones have been added and if the *prefetch* attribute specifies a future time, the acquirer checks and fetches the content or re-crawls the crawl jobs at the time specified by the *prefetch* attribute.

- *expires*

The *expires* attribute is optional and designates a time in yyyy-mm-dd hh:mm:ss format when the content is to be removed from the ECDS network. Additionally, you can specify the GMT time zone. If a time value is omitted, content is stored until it is removed when you modify the relevant Manifest file code.

- *ttl*

The *ttl* attribute is optional and designates a time interval, in minutes, for revalidation of the content. If a time value is omitted, the content is fetched only once and its freshness is never checked again. Usually the *ttl* attribute is a positive value; however, you can also assign a negative value to the *ttl* attribute. The following table describes *ttl* attribute value ranges.

<i>ttl</i> Attribute Value	Action
$ttl > 0$	Content is rechecked every <i>ttl</i> minute. Content is also rechecked if the Manifest file is reparsed and the content specification in the Manifest file has changed or if you click the Refetch button.
$ttl = 0$	Content is fetched only once and never checked again. Content is only rechecked if the Manifest file is reparsed and the content specification in the Manifest file has changed or if you click the Refetch button.
$ttl < 0$	Content is fetched only once and never checked again. Content will <i>not</i> be rechecked if the Manifest file is reparsed or if you click the Refetch button.

- *serveStartTime*

The *serveStartTime* attribute is optional and designates a time in yyyy-mm-dd hh:mm:ss format when the ECDS software is allowed to start serving the content. If the time to serve is omitted, content is ready to serve once it is distributed to the Service Engine or other edge device.

- *serveStopTime*

The *serveStopTime* attribute is optional and designates a time in yyyy-mm-dd hh:mm:ss format when the ECDS software temporarily stops serving the content. If the time to stop serving is omitted, the ECDS software serves the content until it is removed when you modify the relevant Manifest file code.

- *priority*

The *priority* attribute is optional and can be any integer value to specify the content processing priority. If a priority value is omitted, its index order within the Manifest file is used to set the priority.

- *wmtRequireAuth*

The *wmtRequireAuth* attribute is optional and determines whether users need to be authenticated before the specified content is played. When true, the Service Engine requires authentication to play back the specified content to users and communicates with the origin server to check credentials. If the requests pass the credential check, the content is played back from the Service Engine. If this attribute is omitted, a heuristic approach is used to determine the value: if the specified content is acquired by using a username and password, *wmtRequireAuth* is set to true; otherwise, it is set to false. For FTP, if the username is anonymous, *wmtRequireAuth* is set to false.



Note If *wmtRequireAuth* is true, the Origin Server field in the Content Origin page for this delivery service needs to point to the server that can authenticate users. When users want to play back the content, the server specified in the Origin Server field is checked for authentication.

- *failRetryInterval*

The *failRetryInterval* attribute specifies the retry interval, in minutes, when content acquisition fails. For example, *failRetryInterval*="10" means the ECDS software retries content acquisition every 10 minutes after acquisition has failed. If the retry universal value is not specified, the default value is 5 minutes. (The minimum *failRetryInterval* value is accepted.) If a value of less than 5 minutes is specified, that value is converted to 5 minutes.

The behavior differs between failed content acquisition of a single item and failed content acquisition of a crawl item.

- For single item failure:

```
if ( ttl != 0, ttl < retryInterval)
```

The item is rechecked in accordance with the *ttl* attribute. Otherwise, the item is rechecked at the interval specified in the *failRetryInterval* attribute.

- For crawl item failure:

```
if ( ttl != 0 and ttl < retryInterval )
always re-crawl
```

If some items are not acquired (excluding 300 and 400 series status error codes), only failed items are rechecked as specified in the *failRetryInterval* attribute.

When the *ttl* attribute interval occurs, all pages are recrawled.

For example, if *ttl* = 10, and *failRetryInterval* = 4, the following actions occurs:

Number of Minutes	Action
0	Crawl
4	Recheck failed
8	Recheck failed
10	Recrawl
14	Recheck
18	Recheck
20	Recrawl

- *ignoreQueryString*

The *ignoreQueryString* attribute is a playback attribute that can be used with the <options>, <item-group>, <item>, and <crawler> tags. If the value is set to true, then ECDS software ignores any string after a question mark (?) in the request URL for playback. If this attribute is omitted, then the default value is false.

For example, content with the request URL *url=http://web-server/foo* has been prefetched. If a user requests content with the URL *url=http://web-server/foo?id=xxx* and the *ignoreQueryString* attribute value is false, then ECDS software does not use the prefetched content from the request URL *http://web-server/foo*.

However, if the *ignoreQueryString* attribute is set to true, then the ECDS software treats the request URL *http://www-server/foo?id=xxx* the same as *http://www-server/foo* and returns with prefetched content.



Note

How content is cached for dynamic ingests depends on the *ignoreQueryString* value and the protocol engine serving the content.

If the Windows Media Engine is serving the content, and the *ignoreQueryString* is not set, the requested content is cached on the SE. If the *ignoreQueryString* value is set to true, Windows Media Engine caches the content on the SE. If the *ignoreQueryString* value is set to false, the Windows Media Engine does not cache the content on the SE.

The Web Engine only supports the *ignoreQueryString* attribute for pre-positioned content. If the Web Engine is serving the content, and the *ignoreQueryString* attribute is not set, the requested content is not cached on the SE.

- *ignoreOriginPort*

The *ignoreOriginPort* attribute allows playback of prefetched content from a port other than the standard port. If the *ignoreOriginPort* attribute is set to true, content can be played back without regard to the port specified in the request URL. The default for this attribute is false.

This attribute is not intended to be used for content that is routed using a Service Router. It is intended to work only for explicit proxy routing. A typical usage scenario for the *ignoreOriginPort* attribute might be as follows:

- The origin web server is not using port 80; it is using a nonstandard port number in the URL.
- Users are using explicit proxy routing, where the original URL containing the non-standard port number is used for playback from the Service Engine.

Prefetched content cannot be played back using a nonstandard port; prefetched content is served only on ports that are standard for the protocol. If the incoming URL contains a port number other than the protocol's standard port, you must set the *ignoreOriginPort* attribute to true for playback to succeed.

- *userDomainName*

The *userDomainName* attribute is used in two instances: for NTLM authentication and for the SMB file import feature. If the origin server is using NTLM authentication, you must use this attribute to specify the user domain name for NTLM authentication. If a shared folder is protected and the user account is part of a domain, you must use this attribute to specify the domain name of the configured shared folder.

**Note**

Both *userDomainName* and *ntlmUserDomain* cannot coexist in the Manifest file; only one attribute can be used at a time.

- *enableCookies*

The *enableCookies* attribute enables cookie support for the item. When this attribute is set to true, the Content Acquirer, after sending a request for an item to the origin server, parses the server response for cookie name/value pairs. If the server response contains a cookie that is valid and has not expired, the Content Acquirer stores the cookie in main memory.

The Content Acquirer then returns the valid cookie to the server the next time the Content Acquirer sends a request for the item.

A cookie is rejected if it contains any of the following rejection criteria, as found in RFC 2965:

- The value for the Path is not a prefix of the request URI.
For example, if the request is `www.abc.com/aaa/bbb/ccc.html` and the Path of the cookie returned is `/aaa/ccc`, then it is not valid because `/aaa/ccc` is not a prefix of `/aaa/bbb/ccc [URL]`.
- The value for the Domain contains no embedded dots or does not start with a dot.
- The value for the request host is not a domain-match of the Domain.
- The request host is a FQDN (not an IP address) and has the form `HD`, where `D` is the value of the Domain and `H` is a string that contains one or more dots.
- The Path is not a prefix match of the request URL.

**Note**

The Content Acquirer does not use persistent memory to store cookies. If the Service Engine is restarted, all cookie information is lost.

The *enableCookies* attribute can be used with the `<item>`, `<crawler>`, `<item-group>`, and `<options>` tags.

- *authCookie*

The *authCookie* attribute enables the processing and sending of authentication cookies for the item. To enable this feature, the *authCookie* attribute must be set to true for the particular item that passes the user credentials and for which the server sends back the authentication cookies.

The *authCookie* attribute can be used with the `<item>` and `<crawler>` tags. For example:

```
<item src=http://abc.com/auth.cgi?id=10000 authCookie="true"/>
```

The following attributes described under the `<host>` tag attributes can also be specified by the `<item>` tag.

- *disableBasicAuth*
- *noProxy*
- *ntlmUserDomain*
- *password*
- *port*
- *proto*
- *proxyServer*
- *sslAuthType*
- *user*
- *uuencoded*

Subelements

- `<contains />`
- `<schedule/>` `<repeat/>`

The `<schedule/>` `<repeat/>` subelement and its attributes specify a time for a recrawl or an item refetch to begin. You can have multiple `<repeat>` subelements under the `<schedule>` subelement. The attributes *time*, *start*, and *end* specify the day of the month or day of the week and the duration of the specified repeat. The *time* attribute is required, whereas *start* and *end* are optional attributes.



Note The `<schedule>` element takes precedence over the *ttl* attribute.

The *time* attribute uses either of the following formats:

time="dom:hh:mm" or

time="dow:hh:mm"

In these formats, dom is the day of the month (0–30), dow is the day of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat, or *), hh is the clock hour (0–23 or *), and mm is the minute (0–59).

For example:

```
<schedule>
  <repeat time="*:*:0" /> <!-- repeat every hour on the hour -->
  <repeat time="*:13:0" /> <!-- repeat at 1300 every day -->
  <repeat time="Sun:2:30" /> <!-- repeat on Sundays at 2:30 -->
  <repeat time="4:2:30" /> <!-- repeat at 2:30 on the fourth day of the month -->
  <repeat time="Mon:*:30" /> <!-- On Monday, repeat every hour at 30 minutes past
    the hour -->
```

```
</schedule>
```

The *start* and *end* attributes use the following format:

start="yyyy-mm-dd hh:mm:ss"

end="yyyy-mm-dd hh:mm:ss"

For example:

```
<CdnManifest>
<item>
  <schedule>
    <repeat time="Sun:02:30" />
    <repeat time="*: *:34" start="2012-09-11 11:11:11 PST" end="2012-09-11 11:11:21
PST" />
    <repeat time="21:02:35" start="2012-09-11 11:11:11 PST" end="2012-09-11
11:11:21 PST" />
    <repeat time="21:02:35" end="2012-09-11 11:11:21 PST" />
  </schedule>
</item>
.
.
.
```

Example

```
<item
  src="index.html"
  server="cisco.com"
  ttl="3000"
/>
```

crawler

The `<crawler>` `</crawler>` tag set supports crawling a website or an FTP server.

Attributes

- *start-url*

The *start-url* attribute is required. It defines the URL at which to start the process of crawling the website or FTP server. It is identical to the *src* attribute used in the `<item>` tag. (See the “src” subsection in the “item” section on page B-30.)

- *host*

The *host* attribute specifies the host name if the starting URL specified in the *start-url* attribute is a relative URL.

- *depth*

The *depth* attribute is optional and defines the link depth to which a website is to be crawled or directory depth to which an FTP server is to be crawled. If the depth is not specified, the default is 20. The following are the general depth values:

- 0—Acquire only the starting URL.
- 1, 2, 3, and so on—Acquire the starting URL and its referred files.
- -1—Infinite or no depth restriction.

Depth is defined as the level of a website or the directory level of an FTP server, where 0 is the starting URL.

- *prefix*

The *prefix* attribute is optional and combines the hostname from the <server> tag with the value of the *prefix* attribute to create a full prefix. Only content with URLs that match the full prefix is acquired, as shown in this example:

```
<server name="xx"> <host name="www.cisco.com" proto="https" port=433 /> </server>
```

and with the following <crawler> tag:

```
prefix="marketing/eng/"
```

The full prefix is “https://www.cisco.com:433/marketing/eng/.” Only URLs that match this prefix are crawled.

If a prefix is omitted, the crawler checks the default full prefix, which is the hostname portion of the URL from the server. In the example, the default full prefix is “https://www.cisco.com:433.”

- *accept*

The *accept* attribute is optional and uses a regular expression to define acceptable URLs to crawl in addition to matching the prefix. For example, *accept*=“stock” means that only URLs that meet two conditions are searched: the URL matches the prefix and contains the string “stock.” (See the [“Writing Common Regular Expressions” section on page B-7](#) for more information on using regular expressions.)

Note the following two key differences between the *accept* attribute and the *prefix* attribute:

- The *prefix* attribute uses an exact string match, while the *accept* attribute uses a regular expression.
- The *prefix* attribute applies to a URL including all its links or subdirectories. However, the *accept* attribute allows the URL and its links and subdirectories to be evaluated separately.

- *reject*

The *reject* attribute is optional and uses a regular expression to reject a URL if it matches the reject regular expression. The reject regular expression is checked after checking for a prefix URL match. If a URL does not match the prefix, it is immediately rejected. If a URL matches the prefix and the reject parameters, it is rejected by the particular reject constraint. (See the [“Writing Common Regular Expressions” section on page B-7](#) for more information on using regular expressions.)

Note the following two key differences between the *reject* attribute and the *prefix* attribute:

- The *prefix* attribute uses an exact string match, while the *reject* attribute uses a regular expression.
- The *prefix* attribute applies to a URL including all its links or subdirectories. However, the *reject* attribute allows the URL and its links and subdirectories to be evaluated separately.

- *max-number*

The *max-number* attribute is optional and specifies the maximum number of crawler job objects that can be acquired.

- *maxTotalSizeInB/KB/MB*

The *maxTotalSizeInB/KB/MB* attribute is optional and specifies the maximum total content size in bytes, kilobytes, or megabytes that this crawler job can acquire. The size attribute can be expressed in megabytes (MB), kilobytes (KB), or bytes (B).

This attribute replaces the *max-size-in-B/KB/MB* attribute, which continues to be supported for backward compatibility only.

- *srcPrefix*

The *srcPrefix* attribute is optional and must be used in conjunction with the *cdnPrefix* attribute to form a relative ECDS network URL. If a *srcPrefix* attribute is not specified, or if the prefix of the relative source URL does not match the *srcPrefix* attribute, then the relative ECDS network URL is the *cdnPrefix* value combined with the relative source URL. For example, if these content objects have the same source URL prefix “acme/pubs/docs/online/Design/” and you want to replace this prefix with a simple “online/,” then specify *srcPrefix*=”acme/pubs/docs/online/Design/” and *cdnPrefix*=”online/.”

- *cdnPrefix*

The *cdnPrefix* attribute is optional and must be used in conjunction with the *srcPrefix* attribute.

- *wmtRequireAuth*

The *wmtRequireAuth* attribute is optional and determines whether users need to be authenticated before the specified content is played. When true, the Service Engine requires authentication to play back the specified content to users and communicates with the origin server to check credentials. If the requests pass the credential check, the content is played back from the Service Engine. If this attribute is omitted, a process of discovery approach is used to determine the value: if the specified content is acquired by using a username and password, *wmtRequireAuth* is set to true; otherwise, it is set to false. For FTP, if the username is anonymous, *wmtRequireAuth* is set to false.



Note

If *wmtRequireAuth* is set to true, the Origin Server field in the Content Origin page for this delivery service needs to point to the server that can authenticate the users. When users want to play back the content, the server specified in the Origin Server field is checked for authentication.

- *externalPrefixes*

The *externalPrefixes* attribute is optional and specifies additional prefixes for crawl jobs to crawl multiple protocols or multiple websites. Prefixes are separated with a bar (|).

- *externalServers*

The *externalServers* attribute is optional and can be used for multiple host crawling jobs where each host has a different user account. This attribute can be used to see to the <host> tag with the proper authentication information.

- *keepExpiredContent*

The *keepExpiredContent* attribute can be used to acquire content during an HTTP or HTTPS crawl that is expired. When this attribute is set to true, expired content is fetched. When this attribute is set to false, expired content is discarded. If this attribute is not specified, the default is false.

- *keepFolder*

The *keepFolder* attribute is used to fetch folders (a folder is indicated when the request URL ends with a forward slash “/”). If this attribute is set to false, folder URLs are not acquired.

- *keepNoCacheContent*

The *keepNoCacheContent* attribute can be used to acquire content during an HTTP or HTTPS crawl that would normally not be cached. When this attribute is set to true, the acquirer fetches the content even though the content contains an HTTP cache control header indicating that the content is not to be cached. If this attribute is not specified, the default is false.

- *keepQueryUrl*

The *keepQueryUrl* attribute can be used to fetch URLs that contain “?” in the URL string. If this attribute is set to true, URLs with “?” are fetched during HTML parsing for a crawl job if the URL meets the other crawling criteria set forth in the Manifest file.

This attribute is useful when you want to acquire content from a database, for example, where multiple files are differentiated in the portion of the URL string after the “?”. When this attribute is not set, the portion of the URL after the “?” is discarded. If multiple URLs are found where the portion of the URL string in front of the “?” is the same, these URLs appear as duplicates, and only the last “duplicate” URL found is fetched.

- *reportBrokenLinks*

The *reportBrokenLinks* attribute is used to report links on an HTML web page that cannot be fetched. If this attribute is set to true, all broken links encountered during a website crawl are reported as errors. This attribute only applies to a website crawl, not to an index crawl. The default is false and broken links are not reported as errors.

The following attributes described under the `<host>` tag attributes can also be specified by the `<crawler>` tag:

- *disableBasicAuth*
- *noProxy*
- *ntlmUserDomain*
- *password*
- *port*
- *proto*
- *proxyServer*
- *sslAuthType*
- *user*
- *uuencoded*

The following attributes described under the `<item>` tag attributes can also be specified by the `<crawler>` tag.

- *authCookie*
- *enableCookies*
- *expires*
- *failRetryInterval*
- *ignoreOriginPort*
- *ignoreQueryString*
- *playServer*
- *prefetch*
- *priority*
- *serveStartTime*
- *serveStopTime*
- *server*
- *ttl*
- *type*
- *userDomainName*

Subelements

- `<matchRule></matchRule>`
- `<schedule><repeat>`

(See the “[item](#)” section on page B-30 for descriptions of the `<schedule><repeat>` subelements.)

Example

```
<server name="cisco">
  <host name="http://www.cisco.com/jobs/" />
</server>
<crawler
  server="cisco"
  start-url="eng/index.html"
  depth="10"
  prefix="eng/"
  reject=".pl"
  maxTotalSizeIn-MB="200"
/>
```

item-group

The `<item-group></item-group>` tag set is used to place shared attributes under one tag so that they can be shared by every `<item>` and `<crawler>` tag within that group. When attributes are shared, it means that attributes can be defined at either the `<item-group>` tag level for group-wide control or on a per `<item>` or per `<crawler>` tag basis. For example, if every `<item>` tag is using the same *server* and *ttl* attributes, you can create an `<item-group>` tag on top of these `<item>` tags and place the *server* and *ttl* attributes in the `<item-group>` tag.

Using shared attributes makes any Manifest file with many `<item>` tags more efficient by consolidating the `<item>` tags with shared attributes. If the same attribute value exists in both the `<item-group>` and `<item>` tags, the value in the `<item>` tag takes precedence over that value in the `<item-group>` tag.

The `<item-group>` tag must be enclosed within the `<CdnManifest>` tag set and contain one or more `<item>` or `<crawler>` tags.

Attributes

If an attribute value is present only at the `<item-group>` tag level, then it is inherited by its inner element in the `<item>` tag. If an attribute value is present in a crawler job, its attributes, whether inherited or owned, are propagated to the content fetched by the crawler job.

The following attributes can be shared across many `<item>` and `<crawler>` tags and are candidates for the `<item-group>` level tag. See the “[item](#)” section on page B-30 for detailed descriptions of the following attributes:

- *cdn-url*
- *enableCookies*
- *expires*
- *failRetryInterval*
- *host*
- *ignoreOriginPort*
- *ignoreQueryString*
- *playServer*
- *prefetch*

- *wmtRequireAuth*
- *serveStartTime*
- *serveStopTime*
- *server*
- *priority*
- *ttl*
- *type*
- *userDomainName*

The following attributes described under the `<host>` tag attributes can also be specified by the `<item-group>` tag.

- *disableBasicAuth*
- *noProxy*
- *ntlmUserDomain*
- *password*
- *port*
- *proto*
- *proxyServer*
- *sslAuthType*
- *user*
- *uuencoded*

Additionally, the following two attributes can be placed within the `<item-group>` tag. See the [“crawler” section on page B-37](#) for a detailed description of the following two attributes:

- *srcPrefix*
- *cdnPrefix*

These two attributes convert the prefix of the *src-url* (content acquisition URL) to the *cdn-url* (publishing URL) for multiple content objects. These content objects are either implicitly specified by multiple `<item>` tags or acquired through a crawler job.

These two attributes can also be specified in the `<crawler>` tag. If you explicitly specify the *srcPrefix* attribute and *cdnPrefix* attribute for an individual `<crawler>` job, the `<crawler>` tag-level specification takes precedence over the `<item-group>` tag-level settings. If you do not specify these attributes for an individual `<crawler>` job, the `<item-group>` tag-level specification is inherited by the `<crawler>` job.

The *srcPrefix* and *cdnPrefix* attributes generate the relative ECDS network URL using the following rules:

- If the *cdn-url* attribute is present in the `<item>` tag, the relative ECDS network URL contains both the *cdnPrefix* attribute plus the *cdn-url* attribute. For example, if *cdnPrefix*=“eng/spec” and *cdn-url*=“e/f.html,” the relative path in the URL is “eng/spec/e/f.html.”
- If the *srcPrefix* attribute is not present in the `<item>` tag, the relative ECDS network URL is the *cdnPrefix* attribute plus the relative source URL.
- If the prefix of the relative source URL does not match the *srcPrefix* attribute, the relative ECDS network URL is the *cdnPrefix* attribute plus the relative source URL.

- To generate a relative ECDS network URL, remove the matched prefix from the relative source URL and replace it with the *cdnPrefix* attribute.

The relative ECDS network URL of `<item>` in the following example is “acme/default.htm.”

```
<item-group cdnPrefix="acme/" >
  <item src="design/index.html" cdn-url="default.html" />
</item-group>
```

In the following example, content objects with the *srcPrefix* attribute, such as “design/plan/,” have the relative ECDS network URL as “acme/” plus relative source URLs stripped of “design/plan/.” Other content objects with a prefix attribute that does not match “design/plan/” have “acme/” plus their original relative source URL.

```
<crawler
  start-url="design/plan/index.html"
  depth="-1"
  srcPrefix="design/plan/"
  cdnPrefix="acme/" />
```

Subelements

- `<crawler></crawler>`
- `<item-group>`
- `<item></item>`
- `<schedule><repeat>`

(See the “[item](#)” section on page B-30 for descriptions of the `<schedule><repeat>` subelements.)

Example

```
<!--grouped content items-->
<item-group server="origin-web-server" type="prepos" ttl="300" cdnPrefix="unicorn/" >
  <item cdn-url="newHQpresentation.rm" src="newHQpresentation.rm" />
  <item cdn-url="animatedlogo.mpg" src="animlogo.mpg" />
  <item cdn-url="companytheme.mp3" src="cotheme.mp3" />
  <item cdn-url="newHQlayout.avi" src="newHQ.mov" />
</item-group>
```

matchRule

The `<matchRule></matchRule>` tag set is optional and defines additional filter rules for crawler jobs. It affects only `<crawler>` tasks and is not used by single `<item>` tags. The crawler parameters defined in the `<crawler></crawler>` tag set determine primarily the scope of a crawl search. If a content object does not meet the criteria specified by the crawler parameter, neither it nor its children are searched.

The `<matchRule>` tag, however, determines only whether or not the content objects should be acquired regardless of the scope of the search. If a web page matches the crawler parameters without the `<matchRule>` feature, its children are searched even though its content objects are not acquired.

In the following crawler job example that uses the `<matchRule>` tag, the entire website is searched, but only files with the .jpg file extension larger than 50 kilobytes are acquired.

```
<crawler start-url="index.html" depth="-1" >
  <matchRule>
    <match minFileSizeIn-KB="50" extension="jpg" />
  </matchRule>
</crawler>
```

The `<matchRule>` element can be nested within an `<item-group>` tag to define group-wide filter rules for `<crawler>` tags contained in the group. It can also be a subelement of a particular `<crawler>` job. The `<crawler>` tag-level setting overrides the `<item-group>` tag-level setting when both tags are present.

If you define criteria locally for individual `<crawler>` jobs, any existing group-level criterion is entirely discarded for that `<crawler>` job. If your `<item-group>` tag match rule is set to A and your `<crawler>` tag specifies another match rule set to B, only B is to be used for the `<crawler>` tag rather than a combination of A and B. You can define at most one `<matchRule>` tag per `<item-group>` tag and at most one `<matchRule>` tag per `<crawler>` tag.

Attributes

None

Subelements

At least one `<match>` tag

match

The `<match>` `</match>` tag is optional and specifies the acquisition criteria of content objects before they can be acquired by ECDS software. Every attribute within a single `<match>` tag has a Boolean AND relationship (to form a logical conjunction) with the other attributes.

You can specify multiple `<match>` tags within the `<matchRule>` tag. The `<match>` tags have a Boolean OR relationship (to form a logical inclusion) with other `<match>` tags. You must specify at least one `<match>` tag per `<matchRule>` tag.

Attributes

- *mime-type*

The *mime-type* attribute specifies MIME-types.

- *extension*

The *extension* attribute specifies file extensions.

- *time-before*

The *time-before* attribute can provide both an absolute time (modified before yyyy-mm-dd hh:mm:ss) or a relative time (modified within ddd:hh:ss), relative to the present time, to download content. Time parameters should be expressed in GMT time zones. (For GMT offsets, see the [“Manifest File Time Zone Tables”](#) section on page B-52.)

- *time-after*

The *time-after* attribute can provide both an absolute time (modified after yyyy-mm-dd hh:mm:ss) or a relative time (modified within ddd:hh:ss), relative to the present time, to download content. Time parameters should be expressed in GMT time zones. (For GMT offsets, see the [“Manifest File Time Zone Tables”](#) section on page B-52.)



Note

Relative time is calculated based on current time. We recommend that you synchronize the server clock and the Service Engine clock so that relative time calculations are accurate.

- *minFileSizeInB/KB/MB*

The *minFileSizeInB/KB/MB* attribute specifies that the acquired content size must be larger than this number of bytes, kilobytes, or megabytes. The size attribute can be expressed in bytes (B), kilobytes (KB), or megabytes (MB).

The *minFileSizeInB/KB/MB* attribute replaces the *size-min-in-B/KB/MB* attribute, which continues to be supported for backward compatibility only.

- *maxFileSizeInB/KB/MB*

The *maxFileSizeInB/KB/MB* attribute specifies that the acquired content size must be smaller than this number of bytes, kilobytes, or megabytes. This attribute can be expressed in bytes (B), kilobytes (KB), or megabytes (MB).

The *maxFileSizeInB/KB/MB* attribute replaces the *size-max-in-B/KB/MB* attribute, which continues to be supported for backward compatibility only.

- *prefix*

The *prefix* attribute is optional and specifies a prefix as a match rule to filter out websites during a crawl job.

- *url-pattern*

The *url-pattern* attribute is optional and specifies a regular expression as a match rule to filter out certain URLs.

Subelements

None

Examples

```
<!-- crawling item group -->
<item-group server="origin-server" type="prepos">
  <matchRule>
    <match time-before="2012-05-05 12:0:0"/>
  </matchRule>
  <crawler start-url="eng/index.html" depth="-1"/>
  <crawler start-url="hr/index.html" depth="3">
    <matchRule>
      <match minFileSizeIn-KB="1" extension="xxx"/>
    </matchRule>
  </crawler>
</item-group>
```

To download content that was created or modified within the last 90 days, use the relative time format, as shown in the following example:

```
<match time-after="90:00:00"/>
```

To download content that was not modified within the last 2 weeks, use the relative time format, as shown in the following example:

```
<match time-before="14:00:00"/>
```

To download content that has been modified after January 30, 2012, 10:30 p.m., use the absolute time format, as shown in the following example:

```
<match time-after="2012-01-30 10:30:00"/>
```

contains

The `<contains />` tag is optional and identifies content objects that are embedded within the content item currently being described. For example, the components of a Synchronized Multimedia Integration Language (SMIL) file request for an item using `<contains />` links are only accepted after ECDS software determines that dependent content objects are present in the Service Engine.

The `<contains />` tag must be enclosed within the `<item>` `</item>` tag.

The `<contains />` tag is used to include embedded files for some video files, such as .asf or .rp. The ECDS software does not serve this item unless every contained item is present.

Attributes

The `cdn-url` attribute is required and is the relative ECDS network URL of one of the embedded contents.

Subelements

None

Example

```
<item src="house/img08.jpj" cdn-url="img08.jpg" />
<item src="house/img09.jpj" cdn-url="img09.jpg" />
<item cdn-url="house.rp" src="house/house.rp">
  <contains cdn-url="img08.jpg" />
  <contains cdn-url="img09.jpg" />
</item>
```

XML Schema

An XML schema defines the custom markup language of the Manifest file and the appearance of a given set of XML documents. The XML schema specifies which tags or elements you can use in your documents, the attributes those tags can contain, and their arrangement.

See the following sections for more information:

- [Manifest XML Schema, page B-46](#)
- [PlayServerTable XML Schema, page B-51](#)
- [Default PlayServerTable Schema, page B-51](#)

Manifest XML Schema

An XSD is a library that provides an application programming interface (API) for manipulating the components of an XML schema.

The following XML code is the Manifest XML schema (CdnManifest.xsd):

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2002/XMLSchema">
<xs:include schemaLocation="PlayServerTable.xsd"/>
<xs:element name="CdnManifest">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="playServerTable" minOccurs="0" maxOccurs="1"/>
      <xs:element ref="options" minOccurs="0" maxOccurs="1"/>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element ref="proxyServer" maxOccurs="unbounded"/>
        <xs:element ref="server" maxOccurs="unbounded">
          <xs:element ref="item-group" maxOccurs="unbounded">
            <xs:element ref="item" maxOccurs="unbounded"/>
            <xs:element ref="crawler" maxOccurs="unbounded"/>
          </xs:choice>
        </xs:element>
      </xs:choice>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```



```

        <xs:element ref="item" maxOccurs="unbounded"/>
        <xs:element ref="crawler" maxOccurs="unbounded"/>
    </xs:choice>
</xs:sequence>
</xs:complexType>
</xs:element>

<xs:element name="options">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="schedule" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
        <xs:attribute name="timeZone" type="xs:string" use="optional"/>
    </xs:complexType>
    <xs:attribute name="wmtRequireAuth" type="xs:boolean" use="optional"/>
    <xs:attribute name="ignoreQueryString" type="xs:boolean" use="optional"/>
    <xs:attribute name="ignoreOriginPort" type="xs:boolean" use="optional"/>
    <xs:attribute name="enableCookies" type="xs:boolean" use="optional"/>
    <xs:attribute name="ttl" type="xs:int" use="optional"/>
    <xs:attribute name="failRetryInterval" type="xs:unsignedInt" use="optional"/>
    <xs:attribute name="prefetch" type="xs:string" use="optional"/>
    <xs:attribute name="type" use="optional" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="prepos"/>
                <xs:enumeration value="wmt-live"/>
                <xs:enumeration value="cache"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="manifest-id" type="xs:string" use="optional"/>
    <xs:attribute name="clearlog" type="xs:boolean" use="optional"/>
    <xs:attribute name="rd" type="xs:string" use="optional"/>
    <xs:attribute name="prepos-tag" type="xs:string" use="optional"/>
    <xs:attribute name="live-tag" type="xs:string" use="optional"/>
</xs:complexType>
</xs:element>

<xs:element name="server">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="host" minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
        <xs:attribute name="name" type="xs:string" use="required"/>
    </xs:complexType>
</xs:element>

<xs:attributeGroup name="hostAttr">
    <xs:attribute name="proxyServer" type="xs:string" use="optional"/>
    <xs:attribute name="noProxy" type="xs:boolean" use="optional"/>
    <xs:attribute name="proto" use="optional">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="http"/>
                <xs:enumeration value="https"/>
                <xs:enumeration value="ftp"/>
                <xs:enumeration value="rtsp"/>
                <xs:enumeration value="file"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="port" type="xs:unsignedShort" use="optional"/>
    <xs:attribute name="user" type="xs:string" use="optional"/>
    <xs:attribute name="password" type="xs:string" use="optional"/>
    <xs:attribute name="ntlmUserDomain" type="xs:string" use="optional"/>

```

```

<xs:attribute name="userDomainName" type="xs:string" use="optional"/>
<xs:attribute name="disableBasicAuth" type="xs:boolean" use="optional"/>
<xs:attribute name="uuencoded" type="xs:boolean" use="optional"/>
<xs:attribute name="sslAuthType" use="optional">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="weak"/>
      <xs:enumeration value="strong"/>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
</xs:attributeGroup>

<xs:element name="host">
  <xs:complexType>
    <xs:attribute name="name" type="xs:string" use="required"/>
    <xs:attributeGroup ref="hostAttr"/>
  </xs:complexType>
</xs:element>

<xs:element name="proxyServer">
  <xs:complexType>
    <xs:attribute name="serverName" type="xs:string" use="required"/>
    <xs:attribute name="host" type="xs:string" use="optional"/>
    <xs:attribute name="port" type="xs:unsignedShort" use="optional"/>
    <xs:attribute name="user" type="xs:string" use="optional"/>
    <xs:attribute name="password" type="xs:string" use="optional"/>
    <xs:attribute name="ntlmUserDomain" type="xs:string" use="optional"/>
    <xs:attribute name="uuencoded" type="xs:string" use="optional"/>
    <xs:attribute name="disableBasicAuth" type="xs:boolean" use="optional"/>
  </xs:complexType>
</xs:element>

<xs:attributeGroup name="contentAttr">
  <xs:attribute name="server" type="xs:string" use="optional"/>
  <xs:attribute name="playServer" type="xs:string" use="optional"/>
  <xs:attribute name="type" use="optional">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="prepos"/>
        <xs:enumeration value="wmt-live"/>
        <xs:enumeration value="cache"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>

  <xs:attribute name="enableCookies" type="xs:boolean" use="optional"/>
  <xs:attribute name="wmtRequireAuth" type="xs:boolean" use="optional"/>
  <xs:attribute name="ignoreQueryString" type="xs:boolean" use="optional"/>
  <xs:attribute name="ignoreOriginPort" type="xs:boolean" use="optional"/>
  <xs:attribute name="ttl" type="xs:int" use="optional"/>
  <xs:attribute name="failRetryInterval" type="xs:unsignedInt" use="optional"/>
  <xs:attribute name="priority" type="xs:unsignedInt" use="optional"/>
  <xs:attribute name="prefetch" type="xs:string" use="optional"/>
  <xs:attribute name="expires" type="xs:string" use="optional"/>
  <xs:attribute name="serve" type="xs:string" use="optional"/>
  <xs:attribute name="serveStartTime" type="xs:string" use="optional"/>
  <xs:attribute name="serveStopTime" type="xs:string" use="optional"/>
  <xs:attribute name="_isDefault" type="xs:boolean" use="optional"/>
</xs:attributeGroup>

<xs:attributeGroup name="prefixAttr">
  <xs:attribute name="cdnPrefix" type="xs:string" use="optional"/>
  <xs:attribute name="srcPrefix" type="xs:string" use="optional"/>

```

```

</xs:attributeGroup>

<xs:element name="item-group">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="matchRule" minOccurs="0" maxOccurs="1"/>
      <xs:element ref="schedule" minOccurs="0" maxOccurs="1"/>
      <xs:choice minOccurs="1" maxOccurs="unbounded">
        <xs:element ref="item-group" maxOccurs="unbounded"/>
        <xs:element ref="item" maxOccurs="unbounded"/>
        <xs:element ref="crawler" maxOccurs="unbounded"/>
      </xs:choice>
    </xs:sequence>
    <xs:attributeGroup ref="contentAttr"/>
    <xs:attributeGroup ref="prefixAttr"/>
    <xs:attribute name="host" type="xs:string" use="optional"/>
    <xs:attributeGroup ref="hostAttr"/>
  </xs:complexType>
</xs:element>

<xs:element name="item">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="contains" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element ref="schedule" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute name="src" type="xs:string" use="required"/>
    <xs:attribute name="cdn-url" type="xs:string" use="optional"/>
    <xs:attributeGroup ref="contentAttr"/>
    <xs:attribute name="host" type="xs:string" use="optional"/>
    <xs:attribute name="authCookie" type="xs:boolean" use="optional" />
    <xs:attributeGroup ref="hostAttr"/>
  </xs:complexType>
</xs:element>

<xs:element name="crawler">
  <xs:complexType>
    <xs:all>
      <xs:element ref="matchRule" minOccurs="0" maxOccurs="1"/>
      <xs:element ref="schedule" minOccurs="0" maxOccurs="1"/>
    </xs:all>
    <xs:attribute name="start-url" type="xs:string" use="required"/>
    <xs:attribute name="externalPrefixes" type="xs:string" use="optional"/>
    <xs:attribute name="externalServers" type="xs:string" use="optional"/>
    <xs:attribute name="keepFolder" type="xs:boolean" use="optional" />
    <xs:attribute name="keepQueryUrl" type="xs:boolean" use="optional" />
    <xs:attribute name="keepNoCacheContent" type="xs:boolean" use="optional" />
    <xs:attribute name="keepExpiredContent" type="xs:boolean" use="optional" />
    <xs:attribute name="depth" type="xs:short" use="optional"/>
    <xs:attribute name="prefix" type="xs:string" use="optional"/>
    <xs:attribute name="accept" type="xs:string" use="optional"/>
    <xs:attribute name="reject" type="xs:string" use="optional"/>
    <xs:attribute name="max-number" type="xs:unsignedInt" use="optional"/>
    <xs:attribute name="reportBrokenLinks" type="xs:boolean" use="optional" />
    <xs:attribute name="maxTotalSizeIn-B" type="xs:unsignedInt" use="optional"/>
    <xs:attribute name="maxTotalSizeIn-KB" type="xs:unsignedInt" use="optional"/>
    <xs:attribute name="maxTotalSizeIn-MB" type="xs:unsignedInt" use="optional"/>
    <xs:attribute name="maxTotalSizeInB" type="xs:unsignedInt" use="optional"/>
    <xs:attribute name="maxTotalSizeInKB" type="xs:unsignedInt" use="optional"/>
    <xs:attribute name="maxTotalSizeInMB" type="xs:unsignedInt" use="optional"/>
    <xs:attributeGroup ref="contentAttr"/>
    <xs:attributeGroup ref="prefixAttr"/>
    <xs:attribute name="host" type="xs:string" use="optional"/>
    <xs:attribute name="authCookie" type="xs:boolean" use="optional" />

```

```

        <xs:attributeGroup ref="hostAttr"/>
    </xs:complexType>
</xs:element>

<xs:element name="contains">
    <xs:complexType>
        <xs:attribute name="cdn-url" type="xs:string" use="required"/>
    </xs:complexType>
</xs:element>

<xs:element name="matchRule">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="match" minOccurs="1" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="match">
    <xs:complexType>
        <xs:attribute name="mime-type" type="xs:string" use="optional"/>
        <xs:attribute name="time-before" type="xs:string" use="optional"/>
        <xs:attribute name="time-after" type="xs:string" use="optional"/>
        <xs:attribute name="minFileSizeIn-B" type="xs:int" use="optional"/>
        <xs:attribute name="maxFileSizeIn-B" type="xs:int" use="optional"/>
        <xs:attribute name="minFileSizeIn-KB" type="xs:int" use="optional"/>
        <xs:attribute name="maxFileSizeIn-KB" type="xs:int" use="optional"/>
        <xs:attribute name="minFileSizeIn-MB" type="xs:int" use="optional"/>
        <xs:attribute name="maxFileSizeIn-MB" type="xs:int" use="optional"/>
        <xs:attribute name="minFileSizeInB" type="xs:int" use="optional"/>
        <xs:attribute name="maxFileSizeInB" type="xs:int" use="optional"/>
        <xs:attribute name="minFileSizeInKB" type="xs:int" use="optional"/>
        <xs:attribute name="maxFileSizeInKB" type="xs:int" use="optional"/>
        <xs:attribute name="minFileSizeInMB" type="xs:int" use="optional"/>
        <xs:attribute name="maxFileSizeInMB" type="xs:int" use="optional"/>
        <xs:attribute name="extension" type="xs:string" use="optional"/>
        <xs:attribute name="prefix" type="xs:string" use="optional"/>
        <xs:attribute name="url-pattern" type="xs:string" use="optional"/>
    </xs:complexType>
</xs:element>

<xs:element name="schedule">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="repeat" minOccurs="1" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="repeat">
    <xs:complexType>
        <xs:attribute name="time" type="xs:string" use="required"/>
        <xs:attribute name="start" type="xs:string" use="optional"/>
        <xs:attribute name="end" type="xs:string" use="optional"/>
    </xs:complexType>
</xs:element>
</xs:schema>

```

PlayServerTable XML Schema

The following XML code defines the PlayServerTable schema (playServerTable.xsd) for the CdnManifest.xsd:

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2012/XMLSchema">
  <xs:element name="playServerTable">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="playServer" minOccurs="1" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="playServer">
    <xs:complexType>
      <xs:choice minOccurs="1" maxOccurs="unbounded">
        <xs:element ref="contentType"/>
        <xs:element ref="extension"/>
      </xs:choice>
      <xs:attribute name="name" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="wmt"/>
            <xs:enumeration value="http"/>
            <xs:enumeration value="qtss"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>
  <xs:element name="contentType">
    <xs:complexType>
      <xs:attribute name="name" type="xs:string" use="required"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="extension">
    <xs:complexType>
      <xs:attribute name="name" type="xs:string" use="required"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Default PlayServerTable Schema

The following XML code defines the default PlayServerTable:

```
<?xml version="1.0"?>

<playServerTable xmlns:xsi = "http://www.w3.org/2012/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation = "PlayServerTable.xsd">

  <!-- playServer http and https can always play all prepositon
  contents unless users use customized <playServerTable>
  or "playServer" attribute in the manifest file
  -->

  <playServer name="qtss">
    <contentType name="video/quicktime" />
    <extension name="mov" />
    <extension name="qt" />
```

```

<extension name="mp4" />
<extension name="3gp" />
<extension name="3g2" />

<!-- extension avi could also go here -->
</playServer>

<playServer name="wmt">
  <!-- MIME types taken from
  http://msdn.microsoft.com/workshop/imedia/windowsmedia/server/mime.asp
  -->
  <contentType name="video/x-ms-asf" />
  <contentType name="audio/x-ms-wma" />
  <contentType name="video/x-ms-wmv" />
  <contentType name="video/x-ms-wm" />
  <contentType name="application/x-ms-wmz" />
  <contentType name="application/x-ms-wmd" />

  <extension name="wma" /> <!-- audio content -->
  <extension name="wmv" /> <!-- audio/video content -->
  <extension name="asf" /> <!-- audio/video content (legacy) -->
  <extension name="wm" /> <!-- reserved for future use -->

</playServer>
</playServerTable>

```

Manifest File Time Zone Tables

To convert to local time, you must know the time difference between Greenwich mean time (GMT) and local time for both standard time and summer time (daylight saving time). The format for writing the time zone is:

`<zonenumber>:[+|-:]hh:mm` per line

In this format, `<zonenumber>` is the name of the time zone or standard time zone abbreviation (see [Table B-6](#)) without spaces before or after the colon (“:”), and “[+|-:]hh:mm” is the GMT offset in hours and minutes. The GMT offset default is “+.”

See the following sections for more information:

- [Standard Time Zones and GMT Offsets, page B-52](#)
- [GMT Offsets by Country, page B-53](#)

Standard Time Zones and GMT Offsets

[Table B-6](#) lists time zones and offsets supported by the Manifest file.

Table B-6 *Standard Time Zones and GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
ACT:+:09:30	Etc/GMT+7:-:07:00	HST:-:10:00
ADT:-:03:00	Etc/GMT+8:-:08:00	IET:-:05:00
AET:+:10:00	Etc/GMT+9:-:09:00	IST:+:05:30
AGT:-:03:00	Etc/GMT-0:00:00	JST:+:09:00

Table B-6 *Standard Time Zones and GMT Offsets (continued)*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
ART:+:02:00	Etc/GMT-10:+:10:00	MDT:-:06:00
AST:-:09:00	Etc/GMT-11:+:11:00	MET:+:01:00
BET:-:03:00	Etc/GMT-12:+:12:00	MIT:-:11:00
BST:+:06:00	Etc/GMT-13:+:13:00	MST7MDT:-:07:00
CAT:+:02:00	Etc/GMT-14:+:14:00	MST:-:07:00
CDT:-:05:00	Etc/GMT-1:+:01:00	NET:+:04:00
CET:+:01:00	Etc/GMT-2:+:02:00	NST:+:12:00
CNT:-:03:30	Etc/GMT-3:+:03:00	NZ-CHAT:+:12:45
CST6CDT:-:06:00	Etc/GMT-4:+:04:00	NZ:+:12:00
CST:-:06:00	Etc/GMT-5:+:05:00	Navajo:-:07:00
CTT:+:08:00	Etc/GMT-6:+:06:00	PDT:-:07:00
EAT:+:03:00	Etc/GMT-7:+:07:00	PLT:+:05:00
ECT:+:01:00	Etc/GMT-8:+:08:00	PNT:-:07:00
EDT:-:04:00	Etc/GMT-9:+:09:00	PRC:+:08:00
EET:+:02:00	Etc/GMT0:00:00	PRT:-:04:00
EST5EDT:-:05:00	Etc/GMT:00:00	PST8PDT:-:08:00
EST:-:05:00	Etc/Greenwich:00:00	PST:-:08:00
Etc/GMT+0:00:00	Etc/UCT:00:00	ROK:+:09:00
Etc/GMT+10:-:10:00	Etc/UTC:00:00	SST:+:11:00
Etc/GMT+11:-:11:00	Etc/Universal:00:00	UCT:00:00
Etc/GMT+12:-:12:00	Etc/Zulu:00:00	UTC:00:00
Etc/GMT+1:-:01:00	GB-Eire:00:00	Universal:00:00
Etc/GMT+2:-:02:00	GB:00:00	VST:+:07:00
Etc/GMT+3:-:03:00	GMT0:00:00	W-SU:+:03:00
Etc/GMT+4:-:04:00	GMT:00:00	WET:00:00
Etc/GMT+5:-:05:00	Greenwich:00:00	Zulu:00:00
Etc/GMT+6:-:06:00	HDT:-:09:00	—

GMT Offsets by Country

See the following sections for GMT offset information listed alphabetically by country:

- [Africa, page B-54](#)
- [America, page B-55](#)
- [Antarctica/Arctic, page B-56](#)
- [Asia, page B-56](#)
- [Atlantic, page B-57](#)

- [Australia, page B-57](#)
- [Brazil, page B-58](#)
- [Canada/Chile/Cuba, page B-58](#)
- [Egypt/Europe, page B-58](#)
- [Hong Kong/Iceland/India/Iran/Israel, page B-59](#)
- [Jamaica/Japan/Kwajalein/Libya, page B-59](#)
- [Mexico/Mideast, page B-60](#)
- [Pacific/Poland/Portugal, page B-60](#)
- [Singapore/System V/Turkey, page B-60](#)
- [U.S., page B-61](#)

Africa

Table B-7 lists time zones and offsets supported by the Manifest file.

Table B-7 Africa GMT Offsets

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Africa/Abidjan:00:00	Africa/Djibouti:+:03:00	Africa/Maputo:+:02:00
Africa/Accra:00:00	Africa/Douala:+:01:00	Africa/Maseru:+:02:00
Africa/Addis_Ababa:+:03:00	Africa/El_Aaiun:00:00	Africa/Mbabane:+:02:00
Africa/Algiers:+:01:00	Africa/Freetown:00:00	Africa/Mogadishu:+:03:00
Africa/Asmera:+:03:00	Africa/Gaborone:+:02:00	Africa/Monrovia:00:00
Africa/Bamako:00:00	Africa/Harare:+:02:00	Africa/Nairobi:+:03:00
Africa/Bangui:+:01:00	Africa/Johannesburg:+:02:00	Africa/Ndjamena:+:01:00
Africa/Banjul:00:00	Africa/Kampala:+:03:00	Africa/Niamey:+:01:00
Africa/Bissau:00:00	Africa/Khartoum:+:03:00	Africa/Nouakchott:00:00
Africa/Blantyre:+:02:00	Africa/Kigali:+:02:00	Africa/Ouagadougou:00:00
Africa/Brazzaville:+:01:00	Africa/Kinshasa:+:01:00	Africa/Porto-Novo:+:01:00
Africa/Bujumbura:+:02:00	Africa/Lagos:+:01:00	Africa/Sao_Tome:00:00
Africa/Cairo:+:02:00	Africa/Libreville:+:01:00	Africa/Timbuktu:00:00
Africa/Casablanca:00:00	Africa/Lome:00:00	Africa/Tripoli:+:02:00
Africa/Ceuta:+:01:00	Africa/Luanda:+:01:00	Africa/Tunis:+:01:00
Africa/Conakry:00:00	Africa/Lubumbashi:+:02:00	Africa/Windhoek:+:01:00
Africa/Dakar:00:00	Africa/Lusaka:+:02:00	—
Africa/Dar_es_Salaam:+:03:00	Africa/Malabo:+:01:00	—

America

Table B-8 lists time zones and offsets supported by the Manifest file.

Table B-8 America GMT Offsets

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
America/Adak:--10:00	America/Grenada:--04:00	America/Noronha:--02:00
America/Anchorage:--09:00	America/Guadeloupe:--04:00	America/North_Dak/Ctr:--06:00
America/Anguilla:--04:00	America/Guatemala:--06:00	America/Panama:--05:00
America/Antigua:--04:00	America/Guayaquil:--05:00	America/Pangnirtung:--05:00
America/Araguaina:--03:00	America/Guyana:--04:00	America/Paramaribo:--03:00
America/Aruba:--04:00	America/Halifax:--04:00	America/Phoenix:--07:00
America/Asuncion:--04:00	America/Havana:--05:00	America/Port-au-Prince:--05:00
America/Atka:--10:00	America/Hermosillo:--07:00	America/Port_of_Spain:--04:00
America/Barbados:--04:00	America/Ind/Indian:--05:00	America/Porto_Acre:--05:00
America/Belem:--03:00	America/Ind/Knox:--05:00	America/Porto_Velho:--04:00
America/Belize:--06:00	America/Ind/Marengo:--05:00	America/Puerto_Rico:--04:00
America/Boa_Vista:--04:00	America/Ind/Vevay:--05:00	America/Rainy_River:--06:00
America/Bogota:--05:00	America/Indianapolis:--05:00	America/Rankin_Inlet:--06:00
America/Bogota:--05:00	America/Inuvik:--07:00	America/Recife:--03:00
America/Buenos_Aires:--03:00	America/Iqaluit:--05:00	America/Regina:--06:00
America/Cambridge_Bay:--07:00	America/Jamaica:--05:00	America/Rio_Branco:--05:00
America/Cancun:--06:00	America/Jujuy:--03:00	America/Rosario:--03:00
America/Caracas:--04:00	America/Juneau:--09:00	America/Santiago:--04:00
America/Catamarca:--03:00	America/Ken/Louisville:--05:00	America/Santo_Domingo:--04:00
America/Cayenne:--03:00	America/Ken/Monticello:--05:00	America/Sao_Paulo:--03:00
America/Cayman:--05:00	America/Knox_IN:--05:00	America/Scoresbysund:--01:00
America/Chicago:--06:00	America/La_Paz:--04:00	America/Shiprock:--07:00
America/Chihuahua:--07:00	America/Lima:--05:00	America/St_Johns:--03:30
America/Cordoba:--03:00	America/Los_Angeles:--08:00	America/St_Lucia:--04:00
America/Costa_Rica:--06:00	America/Louisville:--05:00	America/St_Thomas:--04:00
America/Cuiaba:--04:00	America/Maceio:--03:00	America/St_Vincent:--04:00
America/Curacao:--04:00	America/Managua:--06:00	America/Swift_Current:--06:00
America/Danmarkshavn:00:00	America/Manaus:--04:00	America/Tegucigalpa:--06:00
America/Dawson:--08:00	America/Martinique:--04:00	America/Thule:--04:00
America/Dawson_Creek:--07:00	America/Mazatlan:--07:00	America/Thunder_Bay:--05:00
America/Denver:--07:00	America/Mendoza:--03:00	America/Tijuana:--08:00
America/Detroit:--05:00	America/Menominee:--06:00	America/Tortola:--04:00
America/Dominica:--04:00	America/Merida:--06:00	America/Vancouver:--08:00

Table B-8 *America GMT Offsets (continued)*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
America/Edmonton:-:07:00	America/Mexico_City:-:06:00	America/St_Lucia:-:04:00
America/Eirunepe:-:05:00	America/Miquelon:-:03:00	America/Virgin:-:04:00
America/El_Salvador:-:06:00	America/Monterrey:-:06:00	America/Whitehorse:-:08:00
America/Ensenada:-:08:00	America/Monteideo:-:03:00	America/Winnipeg:-:06:00
America/Fort_Wayne:-:05:00	America/Montreal:-:05:00	America/Yakutat:-:09:00
America/Fortaleza:-:03:00	America/Montserrat:-:04:00	America/Yellowknife:-:07:00
America/Glace_Bay:-:04:00	America/Nassau:-:05:00	America/Virgin:-:04:00
America/Godthab:-:03:00	America/New_York:-:05:00	America/Whitehorse:-:08:00
America/Goose_Bay:-:04:00	America/Nipigon:-:05:00	America/Winnipeg:-:06:00
America/Grand_Turk:-:05:00	America/Nome:-:09:00	America/Tortola:-:04:00

Antarctica/Arctic

Table B-9 lists time zones and offsets supported by the Manifest file.

Table B-9 *Antarctica/Arctic GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Antarctica/Casey:+:08:00	Antarctica/McMurdo:+:12:00	Antarctica/Vostok:+:06:00
Antarctica/Davis:+:07:00	Antarctica/Palmer:-:04:00	Arctic/Longyearbyen:+:01:00
Antarctica/DtDUrville:+:10:00	Antarctica/South_Pole:+:12:00	—
Antarctica/Mawson:+:06:00	Antarctica/Syowa:+:03:00	—

Asia

Table B-10 lists time zones and offsets supported by the Manifest file.

Table B-10 *Asia GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Asia/Aden:+:03:00	Asia/Hong_Kong:+:08:00	Asia/Riyadh87:+:03:07
Asia/Almaty:+:06:00	Asia/Hovd:+:07:00	Asia/Riyadh88:+:03:07
Asia/Amman:+:02:00	Asia/Irkutsk:+:08:00	Asia/Riyadh89:+:03:07
Asia/Anadyr:+:12:00	Asia/Istanbul:+:02:00	Asia/Riyadh:+:03:00
Asia/Aqtau:+:04:00	Asia/Jakarta:+:07:00	Asia/Saigon:+:07:00
Asia/Aqtobe:+:05:00	Asia/Jayapura:+:09:00	Asia/Sakhalin:+:10:00
Asia/Ashgabat:+:05:00	Asia/Jerusalem:+:02:00	Asia/Samarkand:+:05:00
Asia/Ashkhabad:+:05:00	Asia/Kabul:+:04:30	Asia/Seoul:+:09:00
Asia/Baghdad:+:03:00	Asia/Kamchatka:+:12:00	Asia/Shanghai:+:08:00
Asia/Bahrain:+:03:00	Asia/Karachi:+:05:00	Asia/Singapore:+:08:00

Table B-10 Asia GMT Offsets (continued)

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Asia/Baku:+:04:00	Asia/Kashgar:+:08:00	Asia/Taipei:+:08:00
Asia/Bangkok:+:07:00	Asia/Katmandu:+:05:45	Asia/Tashkent:+:05:00
Asia/Beirut:+:02:00	Asia/Krasnoyarsk:+:07:00	Asia/Tbilisi:+:04:00
Asia/Bishkek:+:05:00	Asia/Kuala_Lumpur:+:08:00	Asia/Tehran:+:03:30
Asia/Brunei:+:08:00	Asia/Kuching:+:08:00	Asia/Tel_Aviv:+:02:00
Asia/Calcutta:+:05:30	Asia/Kuwait:+:03:00	Asia/Thimbu:+:06:00
Asia/Choibalsan:+:09:00	Asia/Macao:+:08:00	Asia/Thimphu:+:06:00
Asia/Chongqing:+:08:00	Asia/Magadan:+:11:00	Asia/Tokyo:+:09:00
Asia/Chungking:+:08:00	Asia/Manila:+:08:00	Asia/Ujung_Pandang:+:08:00
Asia/Colombo:+:06:00	Asia/Muscat:+:04:00	Asia/Ulaanbaatar:+:08:00
Asia/Dacca:+:06:00	Asia/Nicosia:+:02:00	Asia/Ulan_Bator:+:08:00
Asia/Damascus:+:02:00	Asia/Novosibirsk:+:06:00	Asia/Urumqi:+:08:00
Asia/Dhaka:+:06:00	Asia/Omsk:+:06:00	Asia/Vientiane:+:07:00
Asia/Dili:+:09:00	Asia/Phnom_Penh:+:07:00	Asia/Vladivostok:+:10:00
Asia/Dubai:+:04:00	Asia/Pontianak:+:07:00	Asia/Yakutsk:+:09:00
Asia/Dushanbe:+:05:00	Asia/Pyongyang:+:09:00	Asia/Yekaterinburg:+:05:00
Asia/Gaza:+:02:00	Asia/Qatar:+:03:00	Asia/Yerevan:+:04:00
Asia/Harbin:+:08:00	Asia/Rangoon:+:06:30	—

Atlantic

Table B-11 lists time zones and offsets supported by the Manifest file.

Table B-11 Atlantic GMT Offsets

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Atlantic/Azores:-:01:00	Atlantic/Faeroe:00:00	Atlantic/South_Georgia:-:02:00
Atlantic/Bermuda:-:04:00	Atlantic/Jan_Mayen:+:01:00	Atlantic/St_Helena:00:00
Atlantic/Canary:00:00	Atlantic/Madeira:00:00	Atlantic/Stanley:-:04:00
Atlantic/Cape_Verde:-:01:00	Atlantic/Reykjavik:00:00	—

Australia

Table B-12 lists time zones and offsets supported by the Manifest file.

Table B-12 Australia GMT Offsets

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Australia/ACT:+:10:00	Australia/LHI:+:10:30	Australia/Queensland:+:10:00
Australia/Adelaide:+:09:30	Australia/Lindeman:+:10:00	Australia/South:+:09:30

Table B-12 *Australia GMT Offsets (continued)*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Australia/Brisbane:+:10:00	Australia/Lord_Howe:+:10:30	Australia/Sydney:+:10:00
Australia/Broken_Hill:+:09:30	Australia/Melbourne:+:10:00	Australia/Tasmania:+:10:00
Australia/Canberra:+:10:00	Australia/NSW:+:10:00	Australia/Victoria:+:10:00
Australia/Darwin:+:09:30	Australia/North:+:09:30	Australia/West:+:08:00
Australia/Hobart:+:10:00	Australia/Perth:+:08:00	Australia/Yancowinna:+:09:30

Brazil

Table B-13 lists time zones and offsets supported by the Manifest file.

Table B-13 *Brazil GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Brazil/Acre:-:05:00	Brazil/East:-:03:00	Brazil/West:-:04:00
Brazil/DeNoronha:-:02:00	—	—

Canada/Chile/Cuba

Table B-14 lists time zones and offsets supported by the Manifest file.

Table B-14 *Canada/Chile/Cuba GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Canada/Atlantic:-:04:00	Canada/Mountain:-:07:00	Canada/Yukon:-:08:00
Canada/Central:-:06:00	Canada/Newfoundland:-:03:30	Chile/Continental:-:04:00
Canada/East-Ssktchwan:-:06:00	Canada/Pacific:-:08:00	Chile/EasterIsland:-:06:00
Canada/Eastern:-:05:00	Canada/Saskatchewan:-:06:00	Cuba:-:05:00

Egypt/Europe

Table B-15 lists time zones and offsets supported by the Manifest file.

Table B-15 *Egypt/Eire/Europe GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Egypt:+:02:00	Europe/Kiev:+:02:00	Europe/Simferopol:+:02:00
Eire:00:00	Europe/Lisbon:00:00	Europe/Skopje:+:01:00
Europe/Amsterdam:+:01:00	Europe/Ljubljana:+:01:00	Europe/Sofia:+:02:00
Europe/Andorra:+:01:00	Europe/London:00:00	Europe/Stockholm:+:01:00
Europe/Athens:+:02:00	Europe/Luxembourg:+:01:00	Europe/Tallinn:+:02:00
Europe/Belfast:00:00	Europe/Madrid:+:01:00	Europe/Tirane:+:01:00
Europe/Belgrade:+:01:00	Europe/Malta:+:01:00	Europe/Tiraspol:+:02:00

Table B-15 *Egypt/Eire/Europe GMT Offsets (continued)*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Europe/Berlin:+:01:00	Europe/Minsk:+:02:00	Europe/Uzhgorod:+:02:00
Europe/Bratislava:+:01:00	Europe/Monaco:+:01:00	Europe/Vaduz:+:01:00
Europe/Brussels:+:01:00	Europe/Moscow:+:03:00	Europe/Vatican:+:01:00
Europe/Bucharest:+:02:00	Europe/Nicosia:+:02:00	Europe/Vienna:+:01:00
Europe/Budapest:+:01:00	Europe/Oslo:+:01:00	Europe/Vilnius:+:02:00
Europe/Chisinau:+:02:00	Europe/Paris:+:01:00	Europe/Warsaw:+:01:00
Europe/Copenhagen:+:01:00	Europe/Prague:+:01:00	Europe/Zagreb:+:01:00
Europe/Dublin:00:00	Europe/Riga:+:02:00	Europe/Zaporozhye:+:02:00
Europe/Gibraltar:+:01:00	Europe/Rome:+:01:00	Europe/Zurich:+:01:00
Europe/Helsinki:+:02:00	Europe/Samara:+:04:00	Europe/Simferopol:+:02:00
Europe/Istanbul:+:02:00	Europe/San_Marino:+:01:00	Europe/Skopje:+:01:00
Europe/Kaliningrad:+:02:00	Europe/Sarajevo:+:01:00	Europe/Sofia:+:02:00

Hong Kong/Iceland/India/Iran/Israel

Table B-16 lists time zones and offsets supported by the Manifest file.

Table B-16 *Hong Kong/Iceland/India/Iran/Israel GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Hongkong:+:08:00	Indian/Cocos:+:06:30	Indian/Mauritius:+:04:00
Iceland:00:00	Indian/Comoro:+:03:00	Indian/Mayotte:+:03:00
Indian/Antananarivo:+:03:00	Indian/Kerguelen:+:05:00	Indian/Reunion:+:04:00
Indian/Chagos:+:06:00	Indian/Mahe:+:04:00	Iran:+:03:30
Indian/Christmas:+:07:00	Indian/Maldives:+:05:00	Israel:+:02:00

Jamaica/Japan/Kwajalein/Libya

Table B-17 lists time zones and offsets supported by the Manifest file.

Table B-17 *Jamaica/Japan/Kwajalein/Libya GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Jamaica:-:05:00	Kwajalein:+:12:00	Libya:+:02:00
Japan:+:09:00	—	—

Mexico/Mideast

Table B-18 lists time zones and offsets supported by the Manifest file.

Table B-18 *Mexico/Mideast GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Mexico/BajaNorte:-:08:00	Mexico/General:-:06:00	Mideast/Riyadh88:+:03:07
Mexico/BajaSur:-:07:00	Mideast/Riyadh87:+:03:07	Mideast/Riyadh89:+:03:07

Pacific/Poland/Portugal

Table B-19 lists time zones and offsets supported by the Manifest file.

Table B-19 *Pacific/Poland/Portugal GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Pacific/Apia:-:11:00	Pacific/Johnston:-:10:00	Pacific/Ponape:+:11:00
Pacific/Auckland:+:12:00	Pacific/Kiritimati:+:14:00	Pacific/Port_Moresby:+:10:00
Pacific/Chatham:+:12:45	Pacific/Kosrae:+:11:00	Pacific/Rarotonga:-:10:00
Pacific/Easter:-:06:00	Pacific/Kwajalein:+:12:00	Pacific/Saipan:+:10:00
Pacific/Efate:+:11:00	Pacific/Majuro:+:12:00	Pacific/Samoa:-:11:00
Pacific/Enderbury:+:13:00	Pacific/Marquesas:-:09:30	Pacific/Tahiti:-:10:00
Pacific/Fakaofu:-:10:00	Pacific/Midway:-:11:00	Pacific/Tarawa:+:12:00
Pacific/Fiji:+:12:00	Pacific/Nauru:+:12:00	Pacific/Tongatapu:+:13:00
Pacific/Funafuti:+:12:00	Pacific/Niue:-:11:00	Pacific/Truk:+:10:00
Pacific/Galapagos:-:06:00	Pacific/Norfolk:+:11:30	Pacific/Wake:+:12:00
Pacific/Gambier:-:09:00	Pacific/Noumea:+:11:00	Pacific/Wallis:+:12:00
Pacific/Guadalcanal:+:11:00	Pacific/Pago_Pago:-:11:00	Pacific/Yap:+:10:00
Pacific/Guam:+:10:00	Pacific/Palau:+:09:00	Poland:+:01:00
Pacific/Honolulu:-:10:00	Pacific/Pitcairn:-:08:00	Portugal:00:00

Singapore/System V/Turkey

Table B-20 lists time zones and offsets supported by the Manifest file.

Table B-20 *Singapore/System V/Turkey GMT Offsets*

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
Singapore:+:08:00	SystemV/EST5:-:05:00	SystemV/PST8PDT:-:08:00
SystemV/AST4:-:04:00	SystemV/EST5EDT:-:05:00	SystemV/YST9:-:09:00
SystemV/AST4ADT:-:04:00	SystemV/MST7:-:07:00	SystemV/YST9YDT:-:09:00
SystemV/CST6:-:06:00	SystemV/MST7MDT:-:07:00	Turkey:+:02:00
SystemV/CST6CDT:-:06:00	SystemV/PST8:-:08:00	—

U.S.

Table B-21 lists time zones and offsets supported by the Manifest file.

Table B-21 U.S. GMT Offsets

Time Zone: GMT Offset	Time Zone: GMT Offset	Time Zone: GMT Offset
US/Alaska:-:09:00	US/Eastern:-:05:00	US/Pacific-New:-:08:00
US/Aleutian:-:10:00	US/Hawaii:-:10:00	US/Pacific:-:08:00
US/Arizona:-:07:00	US/Indiana-Starke:-:05:00	US/Samoa:-:11:00
US/Central:-:06:00	US/Michigan:-:05:00	—
US/East-Indiana:-:05:00	US/Mountain:-:07:00	—



APPENDIX **C**

Creating Coverage Zone Files

The following sections describe the Coverage Zone file elements and provide several Coverage Zone file examples:

- [Coverage Zone File Elements, page C-1](#)
- [Zero-IP Based Configuration, page C-2](#)
- [Coverage Zone XML Schema, page C-3](#)
- [Coverage Zone File Examples, page C-6](#)



Tip

For information about importing or uploading a Coverage Zone file, see the [“Coverage Zone File Registration” section on page 9-11](#).

For more information about Coverage Zone files, see the [“Coverage Zone File” section on page 1-23](#).

Coverage Zone File Elements

A *Coverage Zone file* is an XML file used to specify a user-defined coverage zone. In this release of ECDS, the Coverage Zone file supports different tags to support network and subnet proximity configurations.

In addition to the coverage zone information, two optional elements are created for documentation purposes:

- Revision value to specify the version of the Coverage Zone file
- Customer name



Note

The coverage zone file is limited to 40,000 entries.

Coverage Zone files can be created using any ASCII text-editing tool. You can use a single coverage zone text-format file to define all the coverage zones for your ECDS network.



Note

The metric value of a default coverage zone is set to 20. If a particular SE is preferred for a user-defined coverage zone, the metric value in the Coverage Zone file should be set to a value less than 20. If a default coverage zone is preferred, then the metric value in the Coverage Zone file should be set to a value greater than 20.

Table C-1 defines the Coverage Zone file elements.

Table C-1 Coverage Zone File Elements

Tag	Element	Value	Description
location	latitude	float	Not used in this release of ECDS
	longitude	float	Not used in this release of ECDS
coverageZone	network	IP address	Coverage zone IP address range.
	SE	Service Engine name (string)	Specifies the Service Engines serving the coverage zone specified in the network element. This can have one or more elements.
	metric	integer	Value indicating the proximity of the Service Engine to the end user. The lower the value, the closer the Service Engine is to the end user.
	location	—	Value indicating the geographical coordinates (latitude and longitude) of the data center.
CDNNetwork	revision	1.0	Not used in this ECDS release.
	customerName	customer name	Not used in this ECDS release.
	coverageZone	—	This can have one or more coverage zones.

Zero-IP Based Configuration

The zero-ip based configuration is a catch-all condition for routing. It is a network entry in the Coverage Zone file defined as 0.0.0.0/0. It matches all client subnets. If the client subnet does not match any of the other network entries in the Coverage Zone file and a 0.0.0.0/0 network entry exists, then the SEs listed for that entry are considered for serving the client request.

Following is an example of the zero-ip based configuration.

```
<?xml version="1.0"?>
<CDNNetwork>
  <revision>1.0</revision>
  <coverageZone>
    <network>3.1.2.18/32</network>
    <SE>U8-MDE1100-1</SE>
    <metric>5</metric>
  </coverageZone>
  <coverageZone>
    <network>3.1.13.10/32</network>
    <SE>U8-MDE1100-2</SE>
    <metric>5</metric>
  </coverageZone>
  <coverageZone>
    <network>0.0.0.0/0</network>
    <SE>U8-MDE1100-3</SE>
    <metric>20</metric>
  </coverageZone>
</CDNNetwork>
```

Coverage Zone XML Schema

The XML Schema file describes and dictates the content of the XML file. The coveragezone.xsd file contains the XML schema.

The following code is the Coverage Zone XML schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2002/XMLSchema">
  <xsd:annotation>
    <xsd:documentation> Revision: 1.0 </xsd:documentation>
  </xsd:annotation>
  <xsd:annotation>
    <xsd:documentation> Schema used to validate Cisco CDS CoverageZone file </xsd:documentation>
  </xsd:annotation>
  <xsd:simpleType name="ipAddressType">
    <xsd:union>
      <!-- IPv4 Address -->
      <!-- Snum = 1*3DIGIT ; representing a decimal integer -->
      <!-- ; value in the range 0 through 255 -->
      <!-- IPv4-address-literal = Snum 3("." Snum) -->
      <xsd:simpleType>
        <xsd:restriction base="xsd:token">
          <xsd:pattern
value="((1?[0-9]?[0-9]|2[0-4][0-9]|25[0-5])\.){3}(1?[0-9]?[0-9]|2[0-4][0-9]|25[0-5])/[0-9]+"/>
          </xsd:restriction>
        </xsd:simpleType>

      <!-- IPv6 Address -->
      <!-- IPv6-hex = 1*4HEXDIG -->
      <!-- IPv6-full = IPv6-hex 7(":" IPv6-hex) -->
      <!-- IPv6-comp = [IPv6-hex *5(":" IPv6-hex)] "::" [IPv6-hex *5(":" IPv6-hex)] -->
      <!-- ; The "::" represents at least 2 16-bit groups of zeros -->
      <!-- ; No more than 6 groups in addition to the "::" may be present -->
      <!-- IPv6v4-full = IPv6-hex 5(":" IPv6-hex) ":" IPv4-address-literal -->
      <!-- IPv6v4-comp = [IPv6-hex *3(":" IPv6-hex)] "::" [IPv6-hex *3(":" IPv6-hex) ":"]
IPv4-address-literal -->
      <!-- ; The "::" represents at least 2 16-bit groups of zeros -->
      <!-- ; No more than 4 groups in addition to the "::" and IPv4-address-literal may be
present -->
      <!-- IPv6-addr = IPv6-full / IPv6-comp / IPv6v4-full / IPv6v4-comp -->
      <xsd:simpleType>
        <!-- IPv6-full = "::" -->
        <xsd:restriction base="xsd:token">
          <xsd:pattern value="::/[0-9]+"/>
        </xsd:restriction>
      </xsd:simpleType>

      <xsd:simpleType>
        <!-- IPv6-full = IPv6-hex 7(":" IPv6-hex) -->
        <xsd:restriction base="xsd:token">
          <xsd:pattern value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){7}/[0-9]+"/>
        </xsd:restriction>
      </xsd:simpleType>

      <xsd:simpleType>
        <!-- IPv6-comp = [IPv6-hex *5(":" IPv6-hex)] "::" [IPv6-hex *5(":" IPv6-hex)] -->
        <!-- An "::" represents at least 2 16-bit groups of zeros -->
        <!-- No more than 6 groups in addition to the "::" may be present. -->
        <xsd:restriction base="xsd:token">
          <xsd:pattern value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){5}::([A-Fa-f0-9]{1,4})?/[0-9]+"/>
        </xsd:restriction>
      </xsd:simpleType>
    </xsd:union>
  </xsd:simpleType>
</xsd:schema>
```

Cisco ECDS 2.5 Software Administration Guide and Online Help

```

        <xsd:pattern
value=" [A-Fa-f0-9]{1,4}::([A-Fa-f0-9]{1,4}){0,2}:(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5
]))\.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\.(((1?[1-9])?[0
-9])|(2[0-4][0-9])|(25[0-5]))/[0-9]+"/>
        </xsd:restriction>
    </xsd:simpleType>

</xsd:union>
</xsd:simpleType>

<xsd:simpleType name="SENameType">
    <xsd:restriction base="xsd:string">
        <xsd:minLength value="1"/>
        <xsd:maxLength value="80"/>
    </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="LatitudeType">
    <xsd:restriction base="xsd:float">
        <xsd:minInclusive value="-90"/>
        <xsd:maxInclusive value="90"/>
    </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="LongitudeType">
    <xsd:restriction base="xsd:float">
        <xsd:minInclusive value="-180"/>
        <xsd:maxInclusive value="180"/>
    </xsd:restriction>
</xsd:simpleType>

<xsd:complexType name="locationType">
    <xsd:sequence>
        <xsd:element name="latitude" type="LatitudeType"/>
        <xsd:element name="longitude" type="LongitudeType"/>
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="coverageZoneType">
    <xsd:sequence>
        <xsd:element name="network" type="ipAddressType" minOccurs="0"/>
        <xsd:element name="location" type="locationType" minOccurs="0"/>
        <xsd:element name="SE" type="SENameType" minOccurs="1" maxOccurs="unbounded"/>
        <xsd:element name="metric" type="xsd:positiveInteger" minOccurs="1" maxOccurs="1"/>
    </xsd:sequence>
</xsd:complexType>

<xsd:element name="CDNNetwork">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="revision" type="xsd:string" minOccurs="0" maxOccurs="1"/>
            <xsd:element name="customerName" type="xsd:string" minOccurs="0" maxOccurs="1"/>
            <xsd:element name="coverageZone" type="coverageZoneType" minOccurs="0" maxOccurs="unbounded"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>

</xsd:schema>

```

Coverage Zone File Examples

The following sections show different Coverage Zone file scenarios:

- [Scenario 1: Coverage Zone with Client Network Only, page C-6](#)
- [Scenario 2: Coverage Zone with Geographical Location of the Datacenter Only, page C-6](#)
- [Scenario 3: Coverage Zone with Client Network and Geographical Location of the Datacenter, page C-7](#)
- [Scenario 4: Coverage Zone for Same Client Network with Different Weighted SEs, page C-8](#)

Scenario 1: Coverage Zone with Client Network Only

```
<?xml version="1.0" ?>
<!-- Coverage Zone data in XML -->
<CDNNetwork>
  <revision>1.0</revision>
  <customerName> Cisco Systems </customerName>
<!-- San Jose Datacenter -->
  <coverageZone>
    <network>192.1.2.0/16</network>
    <SE>MDE-1100-SE1</SE>
    <SE>MDE-1100-SE2</SE>
    <metric>10</metric>
  </coverageZone>
<!-- Chicago Datacenter -->
  <coverageZone>
    <network>192.1.3.0/24</network>
    <SE>MDE-1100-SE3</SE>
    <SE>MDE-1100-SE4</SE>
    <metric>10</metric>
  </coverageZone>
<!-- New York Datacenter -->
  <coverageZone>
    <network>192.1.4.0/24</network>
    <SE>MDE-1100-SE5</SE>
    <SE>MDE-1100-SE6</SE>
    <metric>10</metric>
  </coverageZone>
</CDNNetwork>
```

Scenario 2: Coverage Zone with Geographical Location of the Datacenter Only

```
<?xml version="1.0" ?>
<!-- Coverage Zone data in XML -->
<CDNNetwork>
  <revision>1.0</revision>
  <customerName> Cisco Systems </customerName>
<!-- San Jose Datacenter -->
  <coverageZone>
    <location>
      <latitude>37</latitude>
      <longitude>-122</longitude>
    </location>
    <SE>MDE-1100-SE1</SE>
    <SE>MDE-1100-SE2</SE>
    <metric>10</metric>
```

```

    </coverageZone>
<!-- Chicago Datacenter -->
    <coverageZone>
        <location>
            <latitude>42</latitude>
            <longitude>-88</longitude>
        </location>
        <SE>MDE-1100-SE3</SE>
        <SE>MDE-1100-SE4</SE>
        <metric>10</metric>
    </coverageZone>
<!-- New York Datacenter -->
    <coverageZone>
        <location>
            <latitude>41</latitude>
            <longitude>-74</longitude>
        </location>
        <SE>MDE-1100-SE5</SE>
        <SE>MDE-1100-SE6</SE>
        <metric>10</metric>
    </coverageZone>
</CDNNetwork>

```

Scenario 3: Coverage Zone with Client Network and Geographical Location of the Datacenter

```

<?xml version="1.0" ?>
<!-- Coverage Zone data in XML -->
<CDNNetwork>
    <revision>1.0</revision>
    <customerName> Cisco </customerName>
<!-- San Jose Datacenter -->
    <coverageZone>
        <network>192.1.2.0/16</network>
        <SE>MDE-1100-SE1</SE>
        <SE>MDE-1100-SE2</SE>
        <metric>10</metric>
    </coverageZone>
<!-- Chicago Datacenter -->
    <coverageZone>
        <location>
            <latitude>41</latitude>
            <longitude>-74</longitude>
        </location>
        <SE>MDE-1100-SE3</SE>
        <SE>MDE-1100-SE4</SE>
        <metric>10</metric>
    </coverageZone>
<!-- New York Datacenter -->
    <coverageZone>
        <network>192.1.4.0/24</network>
        <SE>MDE-1100-SE5</SE>
        <SE>MDE-1100-SE6</SE>
        <metric>10</metric>
    </coverageZone>
</CDNNetwork>

```

Scenario 4: Coverage Zone for Same Client Network with Different Weighted SEs

```
<?xml version="1.0" ?>
<!-- Coverage Zone data in XML -->
<CDNNetwork>
  <revision>1.0</revision>
  <customerName>Cisco Systems</customerName>
  <coverageZone>
    <network> 172.31.10.0/12 </network>
    <SE> dmz2-roam </SE>
    <metric> 10 </metric>
  </coverageZone>
  <coverageZone>
    <network> 172.31.10.0/12 </network>
    <SE> dmz2-is </SE>
    <metric> 20 </metric>
  </coverageZone>
</CDNNetwork>
```




APPENDIX **D**

Creating Authorization Service Files

The following sections describe the Authorization Service configuration file used by a delivery service to specify the geographic regions in which client requests are either allowed or denied:

- [Authorization Service Configuration File Elements, page D-1](#)
- [Authorization Service Configuration XML Schema, page D-2](#)
- [Authorization Service Configuration File Example, page D-6](#)

Authorization Service Configuration File Elements

The Authorization Service configuration file is an XML file used to specify the geographic regions that are allowed or denied access to a delivery service.

In addition to the allowed and denied geographical information, two optional elements are created for documentation purposes: a revision value to specify the version of the file and a customer name.

The configuration files can be created using any ASCII text-editing tool. For information about uploading a configuration file, see the [“Configure Authorization Service” section on page 8-8](#).



Note

The country, state, and city names must match what is used by the Geo-Location server. The names are case sensitive.

The pattern, network, and Geo elements are required for each Allow tag and Deny tag.

[Table D-1](#) defines the Authorization Service configuration file elements.

Table D-1 **Authorization Service Configuration File Elements**

Tag	Element	Value	Description
Allow	pattern	file type suffix	Specifies a pattern that the client’s URL request must match. The pattern can be any substring of the client’s URL request. An asterisk (*) means all URLs.
	network	IP address	Specifies the IP address range of the subnet using classless inter-domain routing (CIDR) notation (A.B.C.D/N).
	Geo		Describes the geographic region by country, state, and city.

Table D-1 Authorization Service Configuration File Elements (continued)

Tag	Element	Value	Description
Deny	pattern	file type suffix	Specifies a pattern that the client's URL request must match. The pattern can be any substring of the client's URL request. An asterisk (*) means all URLs.
	network	IP address	Specifies the IP address range of the subnet using classless inter-domain routing (CIDR) notation (A.B.C.D/N).
	Geo		Describes the geographic region by country, state, and city.
Order	—	Allow, Deny	The order in which to apply the allow and deny rules. One of the following: - Allow, Deny - Deny, Allow
Geo	Country name	country name	Specifies the full name of the country.
	State name	state name	Specifies the full name of the state.
	City name	city name	Specifies the full name of the city.
CDSAuthorization	Revision	1.0	The revision of this file.
	CustomerName	customer name	The customer associated with this file.
	Allow	—	The CDSAuthorization tag can have one Allow element.
	Deny	—	The CDSAuthorization tag can have one Deny element.
	Order	—	The CDSAuthorization tag can have one Order element.

Authorization Service Configuration XML Schema

The XML Schema file describes and dictates the content of the XML file. The CDSAuthorization.xsd file contains the XML schema.

The following code is an example of the Authorization Service configuration XML schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2012/XMLSchema">
  <xsd:annotation>
    <xsd:documentation> Revision: 1.0 </xsd:documentation>
  </xsd:annotation>
  <xsd:annotation>
    <xsd:documentation> Schema used to validate Cisco CDS Authorization file
  </xsd:documentation>
  </xsd:annotation>
  <xsd:simpleType name="ipAddressType">
    <xsd:union>
      <!-- IPv4 Address -->
      <!-- Snum = 1*3DIGIT ; representing a decimal integer -->
      <!-- ; value in the range 0 through 255 -->
      <!-- IPv4-address-literal = Snum 3("." Snum) -->
      <xsd:simpleType>
        <xsd:restriction base="xsd:token">
          <xsd:pattern
value="( (1?[0-9]?[0-9]|2[0-4][0-9]|25[0-5])\. ) {3} (1?[0-9]?[0-9]|2[0-4][0-9]|25[0-5]) / [0-9]
+ " />
          </xsd:restriction>
        </xsd:simpleType>
      </xsd:union>
    </xsd:simpleType>
  </xsd:simpleType>

```

```

<!-- IPv6 Address -->
<!-- IPv6-hex = 1*4HEXDIG -->
<!-- IPv6-full = IPv6-hex 7(":" IPv6-hex) -->
<!-- IPv6-comp = [IPv6-hex *5(":" IPv6-hex)] "::" [IPv6-hex *5(":" IPv6-hex)] -->
<!-- ; The "::" represents at least 2 16-bit groups of zeros -->
<!-- ; No more than 6 groups in addition to the "::" may be present -->
<!-- IPv6v4-full = IPv6-hex 5(":" IPv6-hex) ":" IPv4-address-literal -->
<!-- IPv6v4-comp = [IPv6-hex *3(":" IPv6-hex)] "::" [IPv6-hex *3(":" IPv6-hex) ":" ]
IPv4-address-literal -->
<!-- ; The "::" represents at least 2 16-bit groups of zeros -->
<!-- ; No more than 4 groups in addition to the "::" and
IPv4-address-literal may be present -->
<!-- IPv6-addr = IPv6-full / IPv6-comp / IPv6v4-full / IPv6v4-comp -->
<xsd:simpleType>
  <!-- IPv6-full = IPv6-hex 7(":" IPv6-hex) -->
  <xsd:restriction base="xsd:token">
    <xsd:pattern value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){7}/[0-9]+"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType>
  <!-- IPv6-comp = [IPv6-hex *5(":" IPv6-hex)] "::" [IPv6-hex *5(":" IPv6-hex)] -->
  <!-- An "::" represents at least 2 16-bit groups of zeros -->
  <!-- No more than 6 groups in addition to the "::" may be present. -->
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){5}::([A-Fa-f0-9]{1,4}){7}/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
<xsd:simpleType>
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){4}::([A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){7}){7}/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
<xsd:simpleType>
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){3}::([A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){0,2}){7}/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
<xsd:simpleType>
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){2}::([A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){0,3}){7}/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
<xsd:simpleType>
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){1}::([A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){0,4}){7}/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
<xsd:simpleType>
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}::([A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){0,4}){7}/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
<xsd:simpleType>
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}::([A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){0,4}){7}/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>

```

```

<xsd:simpleType>
  <!-- IPv6v4-full = IPv6-hex 5 ":" IPv4-address-literal -->
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){5}:(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\
.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\
.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
<xsd:simpleType>
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){3}:([A-Fa-f0-9]{1,4})?(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\
.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\
.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
<xsd:simpleType>
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){2}:([A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4})?)?(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\
.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\
.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
<xsd:simpleType>
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}:([A-Fa-f0-9]{1,4}){2}:([A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){0,2})?(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\
.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\
.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
<xsd:simpleType>
  <xsd:restriction base="xsd:token">
    <xsd:pattern
value="[A-Fa-f0-9]{1,4}:([A-Fa-f0-9]{1,4}(:[A-Fa-f0-9]{1,4}){0,2})?(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\
.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))\
.(((1?[1-9])?[0-9])|(2[0-4][0-9])|(25[0-5]))/[0-9]+"/>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:union>
</xsd:simpleType>

<xsd:simpleType name="OrderType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Allow"/>
    <xsd:enumeration value="Deny"/>
    <xsd:enumeration value="Allow,Deny"/>
    <xsd:enumeration value="Deny,Allow"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="PatternType">
  <xsd:restriction base="xsd:string">
    <xsd:maxLength value="1024"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:complexType name="CityType">
  <xsd:attribute name="name" use="required">

```

```

        <xsd:simpleType>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="64"/>
            </xsd:restriction>
        </xsd:simpleType>
    </xsd:attribute>
</xsd:complexType>

<xsd:complexType name="StateType">
    <xsd:sequence>
        <xsd:element name="City" type="CityType" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="name" use="required">
        <xsd:simpleType>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="64"/>
            </xsd:restriction>
        </xsd:simpleType>
    </xsd:attribute>
</xsd:complexType>

<xsd:complexType name="CountryType">
    <xsd:sequence>
        <xsd:element name="State" type="StateType" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="name" use="required">
        <xsd:simpleType>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="64"/>
            </xsd:restriction>
        </xsd:simpleType>
    </xsd:attribute>
</xsd:complexType>

<xsd:complexType name="GeoType">
    <xsd:sequence>
        <xsd:element name="Country" type="CountryType" minOccurs="1"
maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="AllowType">
    <xsd:sequence>
        <xsd:element name="Pattern" type="PatternType" maxOccurs="unbounded"/>
        <xsd:choice maxOccurs="unbounded">
            <xsd:element name="Network" type="ipAddressType"/>
            <xsd:element name="Geo" type="GeoType"/>
        </xsd:choice>
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="DenyType">
    <xsd:sequence>
        <xsd:element name="Pattern" type="PatternType" maxOccurs="unbounded"/>
        <xsd:choice maxOccurs="unbounded">
            <xsd:element name="Network" type="ipAddressType"/>
            <xsd:element name="Geo" type="GeoType"/>
        </xsd:choice>
    </xsd:sequence>
</xsd:complexType>

<xsd:element name="CDSAuthorization">
    <xsd:complexType>
        <xsd:sequence>

```

```

        <xsd:element name="Revision" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="CustomerName" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="Allow" type="AllowType" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="Deny" type="DenyType" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="Order" type="OrderType" minOccurs="1" maxOccurs="1"/>
    </xsd:sequence>
</xsd:complexType>
</xsd:element>

</xsd:schema>

```

Authorization Service Configuration File Example

The following is an example of the Authorization Service configuration file.

```

<CDSAuthorization xmlns:xsi="http://www.w3.org/2012/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>ATT</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>1.1.1.1/24</Network>
    <Network>2.2.2.2/24</Network>
    <Network>3.3.3.3/24</Network>
    <Network>4.4.4.4/8</Network>
    <Network>5.5.5.5/24</Network>
    <Geo>
      <Country name="united states">
        <State name="california">
          <City name="san francisco"/>
          <City name="san jose"/>
          <City name="sunnyvale"/>
        </State>
      </Country>
    </Geo>
    <Geo>
      <Country name="united states">
        <State name="california"/>
        <State name="arizona"/>
      </Country>
      <Country name="germany"/>
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Geo>
      <Country name="france"/>
      <Country name="china">
        <State name="ALL">
          </State>
        </Country>
      </Geo>
    </Deny>
  <Order>Allow,Deny</Order>
</CDSAuthorization>

```



APPENDIX **E**

Verifying the Enterprise CDS

The following sections describe steps to test the ECDS using the different media players:

- [Verifying the Web Engine, page E-1](#)
- [Verifying the Windows Media Streaming Engine, page E-7](#)
- [Verifying the Movie Streamer Engine, page E-11](#)
- [Verifying the Flash Media Streaming Engine, page E-19](#)

Devices Used in This Example

The ECDS network topology example used in these procedures consists of the following devices:

- 2 Service Engines (SEs)
 - NE-DEMO-SE1 — Tier 1 location
 - NE-DEMO-SE2 — Tier 2 location
- 1 Service Router (SR)
 - NE-DEMO-SR — Tier 2 location
- 1 Enterprise Content Delivery System Manager (CDSM)
 - NE-DEMO-CDSM

Verifying the Web Engine

Use the information in the following sections to verify the web engine:

- [Verifying Preingested Web Content, page E-1](#)
- [Verifying Dynamically Ingested Web Content, page E-3](#)

Verifying Preingested Web Content

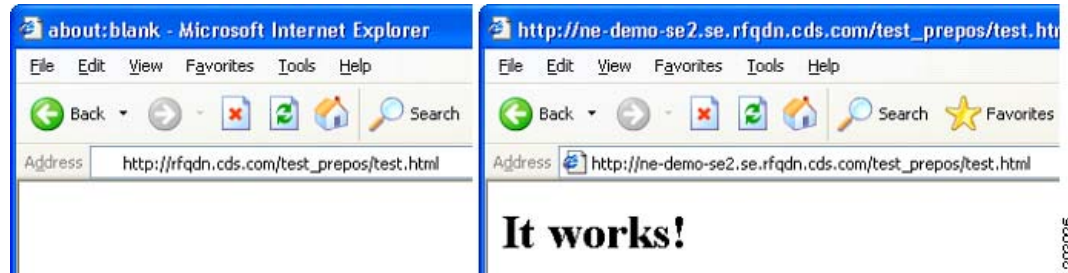
Before You Begin

1. Content must be preingested. See the [“Configuring Delivery Services” section on page 8-1](#) for more information.
2. Verify that the content has been pre-positioned by using the **show distribution object-status name-of-object** command.

Procedure

- Step 1** In a web browser on a client PC, enter the URL of the preingested HTML content using the Service Routing Domain Name in the URL. In the example, this is “http://rfqdn.cds.com/test_prepos/test.html.” Client requests are directed to this domain name and are then redirected by the Service Router to the content on the Service Engine. [Figure E-1](#) shows the initial URL on the left and the redirection on the right.

Figure E-1 URL Redirection for Preingested Content



- Step 2** On the Service Engines, verify that the request was served as a preingested hit. View the HTTP request statistics by starting an SSH session and entering the **show statistics http requests** command. In this case, the Service Router redirected the request to NE-DEMO-SE2, which served the request.

```
NE-DEMO-SE1# show statistics http requests
```

```
Caching Statistics
-----
      Cache Hits : 0
      Cache Miss : 0
      Range Requests : 0
Partial HItS - Live fill : 0
      Partial HIt - Refill : 0
Partial Caching - Bypassed : 0

Prepositioned Content Statistics
-----
      Preposition Hits : 0
      Reply Meta : 0
      Alternate Media : 0

Others
-----
      Num Lookups : 0
      Lookup Errors : 0
Streaming redirected requests : 0
      WMT Liveness requests : 0
Hierarchical Cache Liveness requests : 0

Total      % of requests
-----
Client Errors : 0 0.00
Server Errors : 0 0.00
Http/0.9 Requests : 0 0.00
Http/1.0 Requests : 0 0.00
Http/1.1 Requests : 0 0.00
Http Invalid Requests : 0 0.00
Blocked : 0 0.00
Allowed : 0 0.00
```



```
NE-DEMO-SE2# show statistics http request
```

Caching Statistics

```
-----
          Cache Hits :    0
          Cache Miss :    0
          Range Requests :    0
Partial Hits - Live fill : 0
          Partial HIT - Refill : 0
Partial Caching - Bypassed : 0
```

Prepositioned Content Statistics

```
-----
Preposition Hits : 1
  Reply Meta : 0
  Alternate Media : 0
```

Others

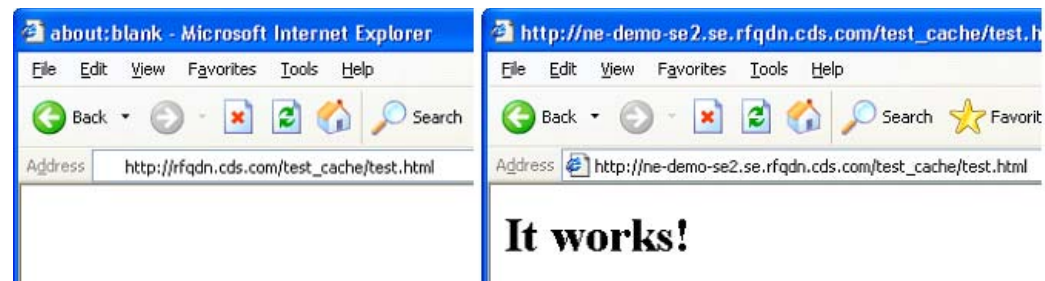
```
-----
          Num Lookups : 1
          Lookup Errors : 0
Streaming redirected requests : 0
          WMT Liveness requests : 0
Hierarchical Cache Liveness requests : 0
```

	Total	% of requests
	-----	-----
Client Errors :	0	0.00
Server Errors :	0	0.00
Http/0.9 Requests :	0	0.00
Http/1.0 Requests :	0	0.00
Http/1.1 Requests :	0	100.00
Http Invalid Requests :	0	0.00
Blocked :	0	0.00
Allowed :	0	100.00

Verifying Dynamically Ingested Web Content

- Step 1** In a web browser on the client PC, enter the URL of non-preingested HTML content on the Service Router. This is content that exists on the origin server or some other server that is accessible but not yet preingested. In the example, the origin server has a directory “test_cache” with a content object “test.html.” [Figure E-2](#) shows the initial URL on the left and the redirection on the right.

Figure E-2 URL Redirection for Non-Preingested Content



This is a cache miss scenario. Neither Service Engine had the content preingested, so the content is acquired by NE-DEMO-SE1 (the Content Acquirer). The content is then cached and replicated to NE-DEMO-SE2 (the receiver, which also happens to be the SE that is serving this client request). NE-DEMO-SE2 then serves the request (as visible by the new URL in [Figure E-2](#)), having cached the content as well.

Step 2 View the HTTP request statistics by entering the **show statistics http requests** command.

```
NE-DEMO-SE1# show statistics http requests
```

```
Caching Statistics
```

```
-----
                Cache Hits : 0
                Cache Miss : 1
                Range Requests : 0
Partial HITs - Live fill : 0
    Partial HIT - Refill : 0
Partial Caching - Bypassed : 0
```

```
Prepositioned Content Statistics
```

```
-----
    Preposition Hits : 0
        Reply Meta : 0
    Alternate Media : 0
        Others
        -----
    Num Lookups : 1
Lookup Errors : 0
Streaming redirected requests : 0
WMT Liveness requests : 0
Hierarchical Cache Liveness requests : 1
```

	Total	% of requests
	-----	-----
Client Errors :	0	0.00
Server Errors :	0	0.00
Http/0.9 Requests :	0	0.00
Http/1.0 Requests :	0	0.00
Http/1.1 Requests :	2	100.00
Http Invalid Requests :	0	0.00
Blocked :	0	0.00
Allowed :	2	100.00

```
NE-DEMO-SE2# show statistics http requests
```

```
Caching Statistics
```

```
-----
                Cache Hits : 0
                Cache Miss : 1
                Range Requests : 0
Partial HITs - Live fill : 0
    Partial HIT - Refill : 0
Partial Caching - Bypassed : 0
```

```
Prepositioned Content Statistics
```

```
-----
    Preposition Hits : 0
        Reply Meta : 0
    Alternate Media : 0
        Others
        -----
    Num Lookups : 1
```

```

Lookup Errors :0
Streaming redirected requests : 0
WMT Liveness requests :0
Hierarchical Cache Liveness requests : 0

```

	Total	% of requests
	-----	-----
Client Errors :	0	0.00
Server Errors :	0	0.00
Http/0.9 Requests :	0	0.00
Http/1.0 Requests :	0	0.00
Http/1.1 Requests :	1	100.00
Http Invalid Requests :	0	0.00
Blocked :	0	0.00
Allowed :	1	100.00

- Step 3** Verify that the content was cached properly on NE-DEMO-SE1 and NE-DEMO-SE2 by entering the **show cache content** command.

```

NE-DEMO-SE1# show cache content
Max-cached-entries is set as 3000000
Number of cal cached assets: 1
-----
Priority   Size    URL
-----
5.41532e-01 44      http://ofqdn.cds.com/test_cache/test.html

```

```

NE-DEMO-SE2#show cache content
Max-cached-entries is set as 3000000
Number of cal cached assets: 1
-----
Priority   Size    URL
-----
6.20339e-01 44      http://ofqdn.cds.com/test_cache/test.html

```

- Step 4** Clear the cache content in the web browser to make sure future requests are handled by the Service Engines instead of from the browser's local cache.

- Step 5** In the web browser, request the same content again (http://rfqdn.cds.com/test_cache/test.html). [Figure E-3](#) shows the initial URL request on the left and the new URL on the right.

Figure E-3 Show Statistic Requests on NE-DEMO-SE1—Cached Content



- Step 6** View the HTTP request statistics again by entering the **show statistics http requests** command.

```

NE-DEMO-SE1# show statistics http requests

Caching Statistics
-----
Cache Hits : 0
Cache Miss : 1
Range Requests : 0
Partial HITs - Live fill : 0

```

```

Partial HIT - Refill : 0
Partial Caching - Bypassed : 0

Prepositioned Content Statistics
-----
Preposition Hits : 0
  Reply Meta : 0
  Alternate Media : 0
  Others
  -----
Num Lookups : 1
Lookup Errors : 0
Streaming redirected requests : 0
WMT Liveness requests : 0
Hierarchical Cache Liveness requests : 1

              Total      % of requests
              -----
Client Errors :      0      0.00
Server Errors :      0      0.00
Http/0.9 Requests : 0      0.00
Http/1.0 Requests : 0      0.00
Http/1.1 Requests : 2     100.00
Http Invalid Requests : 0      0.00
  Blocked :      0      0.00
  Allowed :      2     100.00

NE-DEMO-SE2# show statistics http requests

```

```

Caching Statistics
-----
Cache Hits : 1
Cache Miss : 1
Range Requests : 0
Partial HITs - Live fill : 0
Partial HIT - Refill : 0
Partial Caching - Bypassed : 0

Prepositioned Content Statistics
-----
Preposition Hits : 0
  Reply Meta : 0
  Alternate Media : 0
  Others
  -----
Num Lookups : 2
Lookup Errors : 0
Streaming redirected requests : 0
WMT Liveness requests : 0
Hierarchical Cache Liveness requests : 0

              Total      % of requests
              -----
Client Errors :      0      0.00
Server Errors :      0      0.00
Http/0.9 Requests : 0      0.00
Http/1.0 Requests : 0      0.00
Http/1.1 Requests : 2     100.00
Http Invalid Requests : 0      0.00
  Blocked :      0      0.00
  Allowed :      2     100.00

```

In this case, NE-DEMO-SE2 served the request, and it is a cache hit scenario. The content was cached from the previous attempt, and now the same content is served from cache.

Verifying the Windows Media Streaming Engine

Use the information in the following sections to verify the Windows Media Streaming Engine:

- [Verifying Preingested Windows Media Content, page E-7](#)
- [Verifying Windows Media Live Content Playback, page E-10](#)
- [Verifying Windows Media Live Content Playback](#)

Verifying Preingested Windows Media Content

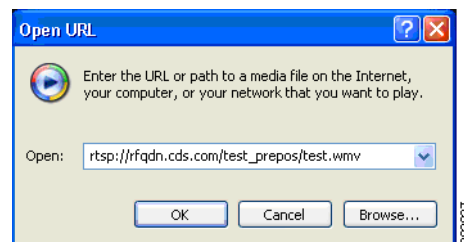
Before You Begin

1. Content must be preingested. See the [“Configuring Delivery Services” section on page 8-1](#) for more information.
2. Verify that the content has been pre-positioned by using the **show distribution object-status name-of-object** command.

Procedure

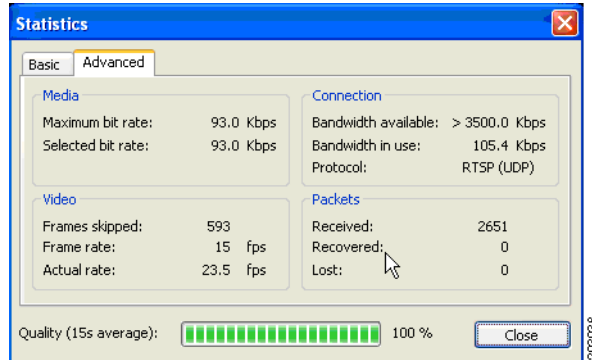
- Step 1** On the client PC, start the Windows Media Player program.
- Step 2** Choose **File > Open URL**.
- Step 3** Enter the URL of the preingested content in the Open URL dialog box ([Figure E-4](#)) and click **OK**. In the example, this is “rtsp://rfqdn.cds.com/test_prepos/test.wmv.”

Figure E-4 Open URL Dialog Box



The video begins to play.

- Step 4** To view the statistics on the video file, choose **View > Statistics** and then click the **Advanced** tab ([Figure E-5](#)).

Figure E-5 Windows Media Player Statistics

- Step 5** To view the request flow, enter the **show statistics wmt streamstat** command on the SEs. In this case, the request is served from NE-DEMO-SE2.

```
NE-DEMO-SE1# show statistics wmt streamstat
Detailed Stream Statistics
```

```
=====
```

```
Incoming Streams:
```

```
=====
```

Stream-Id	Type	Source	State	Bytes-Recd	Duration	Bandwidth	Server-IP	Url-Requested

```
Outgoing Streams:
```

```
=====
```

Client-IP	Type	Transport	Source	State	Pkts-set	Bytes-sent	Duration	BW	Filename	Stream-id

```
NE-DEMO-SE2# show statistics wmt streamstat
Detailed Stream Statistics
```

```
=====
```

```
Incoming Streams:
```

```
=====
```

Stream-Id	Type	Source	State	Bytes-Recd	Duration	Bandwidth	Server-IP	Url-Requested

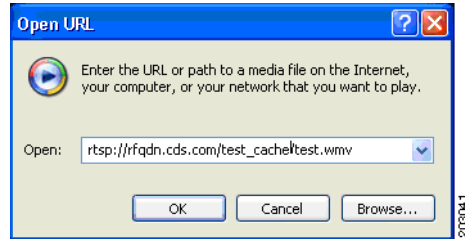
```
Outgoing Streams:
```

```
=====
```

Client-IP	Type	Transport	Source	State	Pkts-set	Bytes-sent	Duration	BW	Filename	Stream-id
171.70.222.171	VOD	NONE	LOCAL	Setup	0	0	0	0	test_prepos/test.wmv	8895

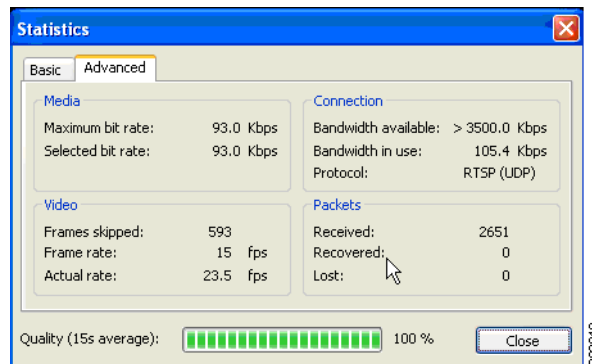
Verifying Dynamically Ingested Windows Media Content

- Step 1** On the client PC, start the Windows Media Player program.
- Step 2** Choose **File > Open URL**.
- Step 3** Enter the URL of content that has not been preingested in the Open URL dialog box (Figure E-6) and click **OK**. In the example, this is “rtsp://rfqdn.cds.com/test_cache/test.wmv.”

Figure E-6 Open URL Dialog Box

The video begins to play.

- Step 4** To view the statistics on the video file, choose **View > Statistics** and then click the **Advanced** tab (Figure E-7).

Figure E-7 Windows Media Player Statistics

- Step 5** To view the request flow, enter the **show statistics wmt streamstat** command on the SEs. In this case, the request is received from NE-DEMO-SE2.

```
NE-DEMO-SE1# clear statistics wmt
NE-DEMO-SE1# show statistics wmt streamstat
Detailed Stream Statistics
=====
```

Incoming Streams:

=====

Stream-Id	Type	Source	State	Bytes-Recd	Duration	Bandwidth	Server-IP	Url-Requested

Outgoing Streams:

=====

Client-IP	Type	Transport	Source	State	Pkts-set	Bytes-sent	Duration	BW	Filename	Stream-id
3.1.4.14	VOD	RTSPT	RMT_HTTP	Play	388	3104000	19	549	test_cache/test.wmv	27521

```
NE-DEMO-SE2# clear statistics wmt
```

```
NE-DEMO-SE2# show statistics wmt streamstat
Detailed Stream Statistics
=====
```

Incoming Streams:

=====

Stream-Id	Type	Source	State	Bytes-Recd	Duration	Bandwidth	Server-IP	Url-Requested
12079	VOD	RMT_RTSP	Play	2241074	23	1550	3.1.4.10	rtsp://ofqdn.cds.com/test_cache/test.wmv

Outgoing Streams:

=====

Client-IP	Type	Transport	Source	State	Pkts-set	Bytes-sent	Duration	BW	Filename	Stream-id
171.70.222.171	VOD	RTSPT	RMT_RTSP	Play	279	2232000	13	7201	test_cache/test.wmv	12043

Verifying Windows Media Live Content Playback

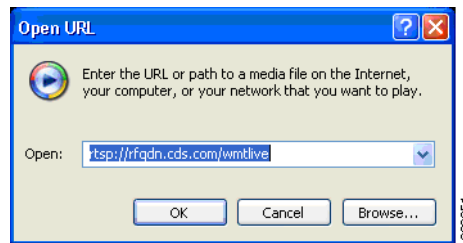


Note

Each live program uses a live delivery service to deliver the live program. See the [“Configuring Programs”](#) section on page 8-25 for more information.

- Step 1** On the client PC, start the Windows Media Player.
- Step 2** Choose **File > Open URL**.
- Step 3** Enter the URL for the live program in the Open URL dialog box (Figure E-8) and click **OK**. In the example, this is “rtsp://rfqdn.cds.com/wmtlive.”

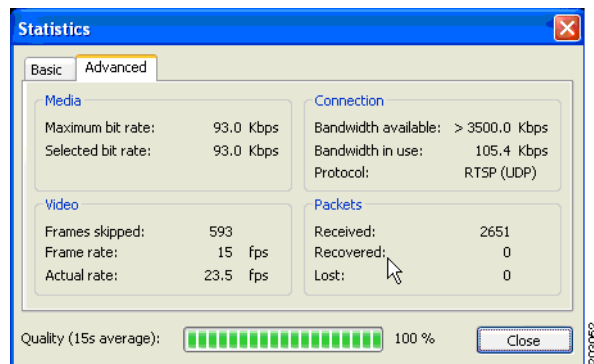
Figure E-8 Open URL Dialog Box



The video begins to play.

- Step 4** To view the statistics on the video file, choose **View > Statistics** and then click the **Advanced** tab (Figure E-9).

Figure E-9 Windows Media Player Statistics



- Step 5** To view the incoming and outgoing streams, enter the **show statistics wmt streamstat** command on the SEs streaming the content. In this case, the request is served from NE-DEMO-SE2.


```

NE-DEMO-SE1# show statistics wmt streamstat
Detailed Stream Statistics
=====

Incoming Streams:
=====
Stream-Id  Type  Source      State  Bytes-Recd  Duration  Bandwidth  Server-IP  Url-Requested
18872      LIVE  RMT_HTTP    Play   84150        241        288        171.70.22.171
http://171.70.222.171:0000

Outgoing Streams:
=====
Client-IP  Type  Transport Source      State Pkts-set  Bytes-sent  Duration  BW  Filename  Stream-id
3.1.4.14   LIVE  RTSPT      RMT_HTTP    Play  5393      7787492     233       288 8080      18889

NE-DEMO-SE2# show statistics wmt streamstat
Detailed Stream Statistics
=====

Incoming Streams:
=====
Stream-Id  Type  Source      State  Bytes-Recd  Duration  Bandwidth  Server-IP  Url-Requested
28772      LIVE  RMT_RTSP    Play   8205265     246        289        3.1.4.10
rtsp://3.1.4.10/wmt_proxy/rtsp&ofqdn.cds.com/wmtlive/___CDS/http&171.70.111.171&8080

Outgoing Streams:
=====
Client-IP  Type  Transport Source      State Pkts-set  Bytes-sent  Duration  BW  Filename  Stream-id
171.70.222.171 LIVE  RTSPU      RMT_RTSP    Play  5582      8060408     241       288 wmtlive  28755

```

Verifying the Movie Streamer Engine

Use the following information to verify the Movie Streamer Engine:

- [Preparing Movie Streamer Content for Ingest, page E-11](#)
- [Verifying Preingested Movie Streamer Content, page E-13](#)
- [Verifying Dynamically Ingested Movie Streamer Content, page E-16](#)
- [Verifying Movie Streamer Live Content Playback, page E-17](#)

Preparing Movie Streamer Content for Ingest

The Movie Streamer delivers hinted MPEG-4, hinted 3GPP, and hinted MOV files to clients over the Internet and mobile networks. Hinted files contain hint tracks, which store packetization information that tell the streaming server how to package content for streaming. Apple QuickTime Pro can be used to generate the hint tracks.

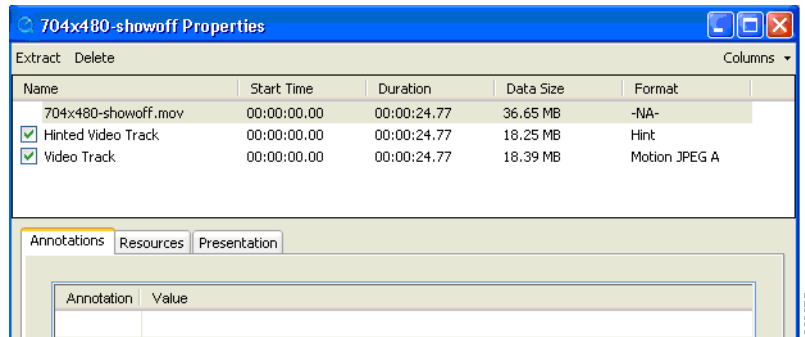


Note

Verify that the content has been pre-positioned by using the **show distribution object-status name-of-object** command.

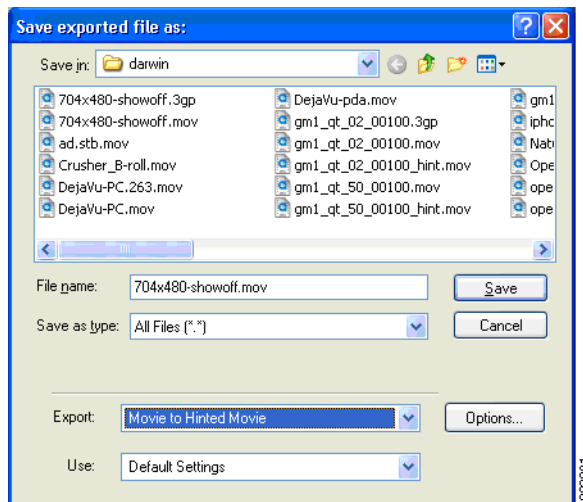
- Step 1** Launch Apple QuickTime Pro.
- Step 2** Choose **File > Open File**, and select a movie file to open.
- Step 3** Choose **Windows > Show Movie Properties**. If there is a Hinted Video Track present, as shown in [Figure E-10](#), then open the next movie file.

Figure E-10 *Movie Properties Dialog Box*

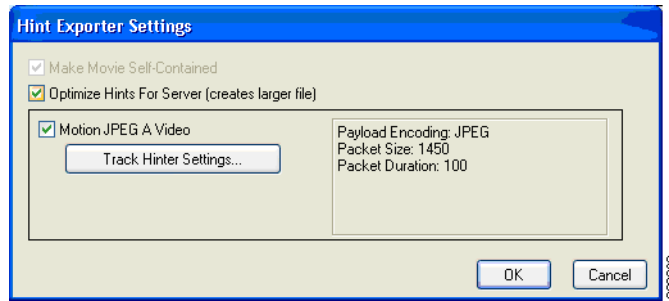


- Step 4** Choose **File > Export**. The Save Exported File dialog box is displayed ([Figure E-11](#)).

Figure E-11 *Save Exported File Dialog Box*



- Step 5** From the **Export** drop-down list, choose **Movie to Hinted Movie**.
- Step 6** Click **Options**. The Hint Exporter Settings dialog box is displayed ([Figure E-12](#)).

Figure E-12 *Hint Exporter Settings Dialog Box*

- Step 7** Check the **Make Movie Self-Contained** check box and the **Optimize Hints For Server** check box.
- Step 8** Click **OK**.
- Step 9** Click **Save** in the Save Exported File dialog box.
- The movie file is ready to be either preingested or dynamically ingested.

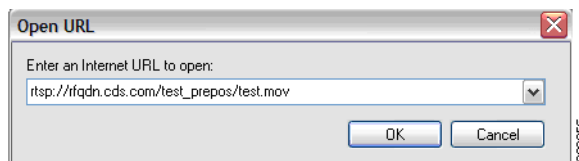
Verifying Preingested Movie Streamer Content

Before You Begin

1. Content must be preingested. See the [“Configuring Delivery Services” section on page 8-1](#) for more information.
2. Verify that the content has been pre-positioned by using the **show distribution object-status name-of-object** command.

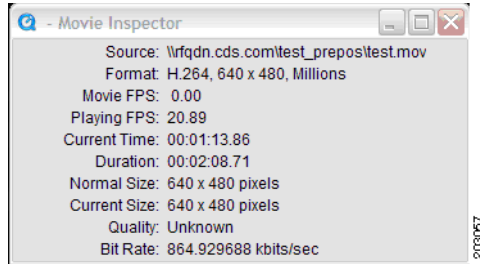
Procedure

- Step 1** On the client PC, start the Apple QuickTime Player.
- Step 2** Choose **File > Open URL**.
- Step 3** Enter the URL of the preingested content in the Open URL dialog box ([Figure E-13](#)) and click **OK**. In the example, this URL is “rtsp://rfqdn.cds.com/test_prepos/test.mov.”

Figure E-13 *Open URL Dialog Box*

The video begins to play.

- Step 4** To view the statistics on the video file, choose **Windows > Show Movie Inspector** ([Figure E-14](#)). The current statistics are displayed and updated as the video streams and plays.

Figure E-14 QuickTime Player Statistics

Step 5 To view the request flow, use the **show statistics movie-streamer all** command.



Note In this example, current connections and bandwidth are all zero because the movie has finished playing at the time the statistics were displayed.

```
NE_DEMO-SE2# show statistics movie-streamer all
Movie Streamer Request Statistics

-----
Current RTSP sessions:                0
Total RTSP sessions:                  0
Current RIP connections:               0
Total RTP connections:                 1

CDN Related Statistics
-----
Preposition Hits:                     1
Cache Hits:                           0
Cache Miss:                           0
Live Requests:                        0

Cache Revalidation Statistics
-----
Fresh Content Requests:                0
Revalidated Requests:                  0

Movie Streamer Bandwidth Usage Statistics
-----
Current Incoming bandwidth:            0 bps
Current Outgoing bandwidth:            0 bps
Current Total bandwidth:                0 bps

Average Incoming bandwidth:            0 bps
Average Outgoing bandwidth:            0 bps
Average Total bandwidth:                0 bps

By Type of Connection
-----
Unicast Incoming Bandwidth:            0 bps
Multicast Incoming Bandwidth:          0 bps
Unicast Outgoing Bandwidth:            0 bps
Multicast Outgoing Bandwidth:          0 bps

By Type of Content
-----
Live Incoming Bandwidth:                0 bps
VOD Incoming Bandwidth:                 0 bps
Live Outgoing Bandwidth:                0 bps
```

```

VOD Outgoing Bandwidth:                0 bps

Overall Traffic
-----
Incoming Bytes:                        0 Bytes
Outgoing Bytes:                       2103939 Bytes
Total Bytes:                          2103939 Bytes

Incoming Packets:                      0
Outgoing Packets:                     1403
Total Packets:                        1403

Movie Streamer Error Statistics
Total
-----
Server Error
-----
Internal Error:                       0
Not Implemented:                      0
Server Unavailable:                   0
Gateway Timeout:                     0
Others:                              0

Client Error
-----
Bad Request:                         0
File Not Found:                      0
Session Not Found:                   0
Method Not Allowed:                  0
Not Enough Bandwidth:                0
Client Forbidden:                    0
Others:                              0

Movie Streamer Performance Statistics
Total
-----
CPU Usage:                           0.000000 %
UpTime:                              5416 sec
Statistics were last cleared on Thursday, 25-Oct-2011 23:53:59 UTC.

```

- Step 6** Play the movie again, and before it completes, display the statistics again.
As the statistics show, there are two current connections: 1 RTP and 1 RTSP.



Note This example shows the full output for the **show statistics** command. All remaining examples for the Movie Streamer statistics show only the relevant information.

```

NE_DEMO-SE2# show statistics movie-streamer all
Movie Streamer Request Statistics
Total
-----
Current RTSP sessions:                1
Total RTSP sessions:                  2
Current RTP connections:               1
Total RTP connections:                 2

CDN Related Statistics
-----
Preposition Hits:                     2
Cache Hits:                           0
Cache Miss:                           0
Live Requests:                        0

```

```

Cache Revalidation Statistics
-----
    Fresh Content Requests:          0
    Revalidated Requests:           0

Movie Streamer Bandwidth Usage Statistics
-----
Current Incoming bandwidth:         0 bps
Current Outgoing bandwidth:         0 bps
Current Total bandwidth:            0 bps

Average Incoming bandwidth:         0 bps
Average Outgoing bandwidth:        863879 bps
Average Total bandwidth:           863879 bps

Incoming Bytes:                     0 Bytes
Outgoing Bytes:                    14490660 Bytes
Total Bytes:                       14490660 Bytes

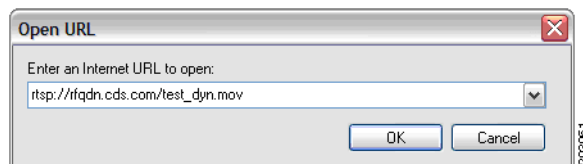
```

Verifying Dynamically Ingested Movie Streamer Content

When content requested by a client is not in the ECDS, it is dynamically ingested from the original source and streamed to the client by an SE.

- Step 1** On the client PC, start the Apple QuickTime Player.
- Step 2** Choose **File > Open URL**.
- Step 3** Enter the URL of a sample MOV file that has not been preingested into the ECDS in the Open URL dialog box ([Figure E-15](#)) and click **OK**. In the example, this is “rtsp://rfqdn.cds.com/test_dyn.mov.”

Figure E-15 Open URL Dialog Box



The video begins to play.

- Step 4** To view the request flow, use the **show statistics movie-streamer all** command.

```

NE_DEMO-SE1# show statistics movie-streamer all
Movie Streamer Request Statistics
-----
Current RTSP sessions:              1
Current RIP connections:            1
Total RTP connections:              4

Movie Streamer Bandwidth Usage Statistics
-----
Current Incoming bandwidth:        207115 bps

```

```

Current Outgoing bandwidth:      0 bps
Current Total bandwidth:        207115 bps

Average Incoming bandwidth:     199244 bps
Average Outgoing bandwidth:     207932 bps
Average Total bandwidth:        407176 bps

Incoming Bytes:                 12667891 Bytes
Outgoing Bytes:                 12609164 Bytes
Total Bytes:                    25277055 Bytes

```

NE_DEMO-SE2# **show statistics movie-streamer all**

```

Movie Streamer Request Statistics
Total
-----
Current RTSP sessions:          0
Current RTP connections:        0
Total RTP connections:          3

Movie Streamer Bandwidth Usage Statistics
Total
-----
Current Incoming bandwidth:     194974 bps
Current Outgoing bandwidth:     0 bps
Current Total bandwidth:        194974 bps

Average Incoming bandwidth:     174557 bps
Average Outgoing bandwidth:     0 bps
Average Total bandwidth:        74557 bps

Incoming Bytes:                 13283705 Bytes
Outgoing Bytes:                 0 Bytes
Total Bytes:                    13283705 Bytes

```

Verifying Movie Streamer Live Content Playback



Note

Each live program uses a live delivery service to deliver the live program. See the [“Configuring Programs” section on page 8-25](#) for more information.

Live streaming of Movie Streamer content requires a Session Description Protocol (SDP) file. The following SDP file is used in this procedure:

```

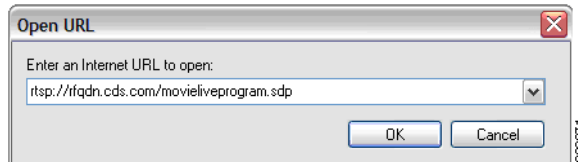
v=0
o=QTSS_Play_List 2079157989 2079176415 IN IP4 171.71.50.216
s=C:\Program Files\Darwin Streaming Server\Playlists\untitled\untitled.sdp
c=IN IP4 127.0.0.1
b=AS:94
t=0 0
a=x-broadcastcontrol:RTSP
m=video 0 RTP/AVP 96
b=AS:79
a=rtpmap:96 X-SV3V-ES/90000
a=control:trackID=1
m=audio 0 RTP/AVP 97
b=AS:14
a=rtpmap:97 X-QDM/22050/2
a=control:trackID=2

```

```
a=x-bufferdelay:4.97
```

- Step 1** On the client PC, start the Apple QuickTime Player.
- Step 2** Choose **File > Open URL**.
- Step 3** Enter the URL of the live program file in the Open URL dialog box (Figure E-16) and click **OK**. In the example, this is “rtsp://rfqdn.cds.com/movieliveprogram.sdp.”

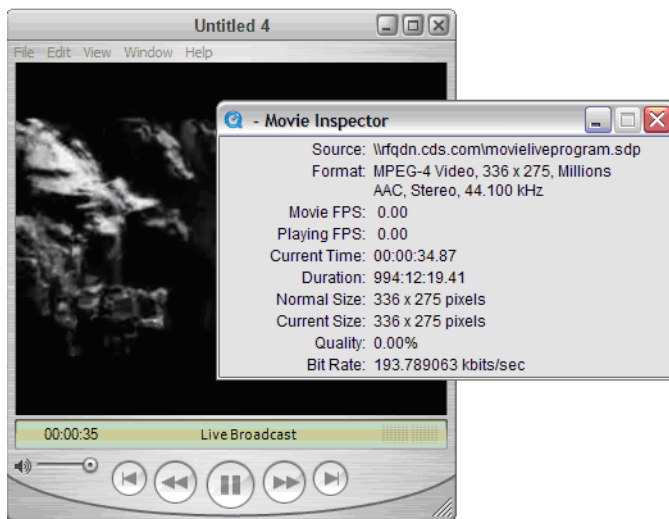
Figure E-16 Open URL Dialog Box



The video begins to play.

- Step 4** To view the statistics on the video file, choose **Window > Show Movie Inspector** (Figure E-17). The current statistics are displayed and updated as the video streams and plays.

Figure E-17 QuickTime Player Statistics



- Step 5** To view the incoming and outgoing streams, use the **show statistics movie-streamer all** command.

```
NE_DEMO-SE1# show statistics movie-streamer all
Movie Streamer Request Statistics
Total
-----
Current RTSP sessions:      1
Current RIP connections:    1
Total RTP connections:      3

Movie Streamer Bandwidth Usage Statistics
Total
-----
Current Incoming bandwidth: 161526 bps
Current Outgoing bandwidth: 582640 bps
```



```

Current Total bandwidth:          744166 bps

Average Incoming bandwidth:       192102 bps
Average Outgoing bandwidth:       203980 bps
Average Total bandwidth:          396082 bps

Incoming Bytes:                   4478769 Bytes
Outgoing Bytes:                   4499370 Bytes
Total Bytes:                      8978139 Bytes

NE_DEMO-SE2# show statistics movie-streamer all
Movie Streamer Request Statistics
Total
-----
Current RTSP sessions:            0
Current RIP connections:          0
Total RTP connections:            1

Movie Streamer Bandwidth Usage Statistics
Total
-----
Current Incoming bandwidth:       175399 bps
Current Outgoing bandwidth:       0 bps
Current Total bandwidth:          175399 bps

Average Incoming bandwidth:       0 bps
Average Outgoing bandwidth:       0 bps
Average Total bandwidth:          0 bps

Incoming Bytes:                   1248165 Bytes
Outgoing Bytes:                   1080984 Bytes
Total Bytes:                      2329149 Bytes

Movie Streamer Performance Statistics
Total
-----
CPU Usage:                        0.000000 %
UpTime:                          78375 sec
Statistics were last cleared on Friday, 26-Oct-2011 20:09:42 UTC.

```

Verifying the Flash Media Streaming Engine

This section consists of the following procedures:

- [Verifying Flash Media Streaming Preingested Content, page E-20](#)
- [Verifying Flash Media Streaming Dynamically Ingested Content, page E-22](#)
- [Verifying Flash Media Streaming—Live Streaming, page E-25](#)

Verifying Flash Media Streaming Preingested Content

**Note**

Content must be preingested. This was accomplished in the “[Configuring Delivery Services](#)” section on [page 8-1](#). Verify that the content has been pre-positioned by using the **show distribution object-status name-of-object** command.

**Note**

Flash Media Streaming uses RTMP to stream live content by dynamic proxy. Configuration of live or rebroadcast programs is not required. When the first client requests live streaming content, the stream is created.

All RTMP calls for live content in the SWF file must be in the following format:

```
rtmp://rfqdn/live-ecds/path/foo.flv
```

In this format, *rfqdn* is the routing domain name of the Service Router, *live* is the required directory, and *path* is the directory path to the content file that conforms to the standard URL specification.

If you are unable to store the VOD content in the required “vod-ecds” directory on your origin server, you can create a VOD virtual path for all RTMP requests. All client requests for RTMP calls still use the `rtmp://rfqdn/vod-ecds/path/foo.flv` format for VOD streams, but the SE replaces the “vod-ecds” directory with the string specified in the **flash-media-streaming application-virtual-path vod-ecds map** command.

Use the **flash-media-streaming application-virtual-path vod-ecds map <mapping string>** command on each SE participating in a Flash Media Streaming delivery service. The mapping string variable accepts all alphanumeric characters and the slash (/) character, and can be from 1 to 128 characters. For example, to map the “vod-ecds” directory to “media” for the go-tv-stream.com origin server, use the **flash-media-streaming application-virtual-path vod-ecds map media** command.

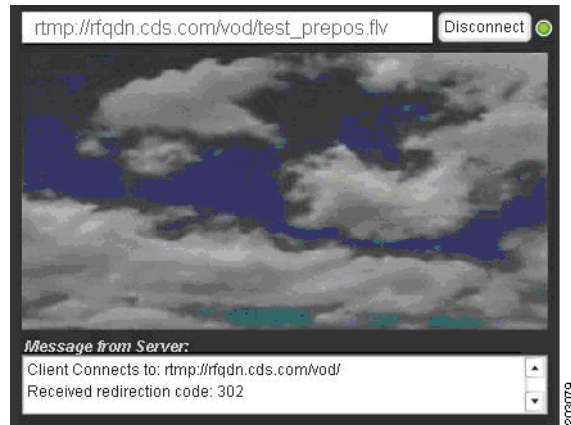
To monitor live streaming, use the **show statistics flash-media-streaming** command and the **show flash-media-streaming livestreams** command.

Step 1 On the client PC, start the Adobe Flash Player.

Step 2 Enter the URL of the flash file in the text box ([Figure E-18](#)) and click **Go**. In the example, this is “`rtmp://rfqdn.cds.com/vod-ecds/test_prepos.flv`.”

The RTMP call is routed to a Service Engine by the Service Router.

The FLV file has been preingested on the SEs. The video begins to play.

Figure E-18 Adobe Flash Player

Step 3 To view the Flash Media Streaming statistics, enter the **show statistics flash-media-streaming** command on the SEs.

There is one concurrent connection on NE-DEMO-SE2, which means there is an active connection to this SE. The statistics also show a Preposition Hit of 1, which means there was preingested content being requested through this SE.

```
NE-DEMO-SE2# show statistics flash-media-streaming
```

```
Flash Media Streaming Statistics
```

```
Statistics were last cleared on Thursday, 06-Dec-2011 37:22:58 UTC.
```

```
Connections
```

```
-----
```

```
Current           : 1
Current VOD       : 1
Current LIVE      : 0
Current DVRCast   : 0
Max Concurrent    : 1
Total             : 1
Total VOD Req     : 0
Total LIVE Req    : 0
Total DVRCast Req : 0
Total Other Proxy Req : 0
```

```
Live Streaming
```

```
-----
```

```
UpStream BW      : 0 kbps
DownStream BW    : 0 kbps
UpStream Bytes   : 0
DownStream Bytes : 0
Num of Instance Load : 0
```

```
DVRCast Streaming
```

```
-----
```

```
UpStream BW      : 0 Kbps
DownStream BW    : 0 Kbps
UpStream Bytes   : 0
DownStream Bytes : 0
Num of Instance Load : 0
```

```
Flash Video Cache Statistics
```

```
-----
```

```
Hits             : 0
Misses           : 0
```

```

Released           :           0
Bytes in cache     :           0
Bytes in use       :           0

Performance
-----
Server Up Time     :      816 S
Mem Usage          :       5 %
Max Mem Usage      :       5 %

Cache
-----
Cache Hit          :       0
Cache Miss         :       0
Proxy Case        :       0
Cache Hit Percentage :    0.00 %

Preposition
-----
Preposition Hit    :       1

Bytes Served
-----
Total Server Bytes :   880668
Local Disk Reads   :       3
HTTP Based Reads   :       0
Bytes From Local Disk : 880668
Bytes Through HTTP :       0

Rules
-----
Action Allow       :       0
Action Block       :       0
Validate url Sign  :       0
Errors             :       0
Auth Server Allow  :       0
Auth Server Deny   :       0

Error
-----
Invalid Error      :       0
Server Error       :       0
Media Not Found    :       0
Media Unauthorized :       0
Invalid Request    :       0

```

Verifying Flash Media Streaming Dynamically Ingested Content



Note

Verifying dynamically ingested content for Flash Media Streaming includes cache miss scenarios and live streaming scenarios. Flash Media Streaming uses RTMP to stream live content by dynamic proxy. Configuration of live or rebroadcast programs is not required. When the first client requests live streaming content, the stream is created.

Step 1 SSH to NE-DEMO-SE1 and use the **show cache content** command to verify there is no cached content.

```
NE-DEMO-SE2# show cache content
Max-cached-entries is set as 3000000
Number of cal cached assets: 0
```

```
-----
Priority      Size      URL
-----
```

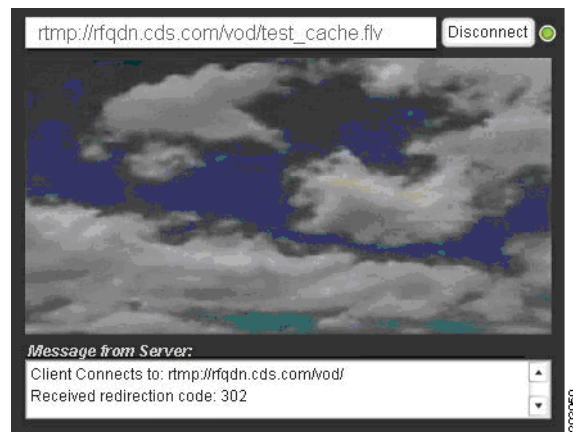
Step 2 On the client PC, start the Adobe Flash Player.

Step 3 Enter the URL of the flash file in the text box (Figure E-19) and click **Go**. In the example, this is “rtmp://rfqdn.cds.com/vod-ecds/test_cache.flv.”

The RTMP call is routed to a Service Engine by the Service Router.

The FLV file has been cached on the SEs. The video begins to play.

Figure E-19 Flash Player



Step 4 To view the Flash Media Streaming statistics, enter the **show statistics flash-media-streaming** command on the SEs.

There is one concurrent connection on NE-DEMO-SE2, which means there is an active connection to this SE. The statistics also show a Cache Miss of 1, which means the content was not found on this SE.

```
NE-DEMO-SE2# show statistics flash-media-streaming
Flash Media Streaming Statistics
Statistics were last cleared on Thursday, 06-Dec-2011 37:22:58 UTC.
```

```
Connections
-----
Current      :      1
Current VOD  :      1
Current LIVE :      0
Max Concurrent :      1
Total        :      1
Total VOD Req :      0
Total LIVE Req :      0
Total DVRCast Req :      0
Total Other Proxy Req :      0

Live Streaming
-----
UpStream BW      :      0 kbps
DownStream BW    :      0 kbps
UpStream Bytes   :      0
DownStream Bytes :      0
```

```

Num of Instance Load :      0

DVRCast Streaming
-----
UpStream BW           :      0 Kbps
DownStream BW         :      0 Kbps
UpStream Bytes        :      0
DownStream Bytes      :      0
Num of Instance Load :      0

Flash Video Cache Statistics
-----
Hits                  :      0
Misses               :      0
Released             :      0
Bytes in cache       :      0
Bytes in use         :      0

Performance
-----
Server Up Time      :      933 S
Mem Usage           :      5 %
Max Mem Usage       :      5 %

Cache
-----
Cache Hit           :      0
Cache Miss          :      1
Proxy Case          :      0
Cache HIT Percentage:  0.00 %

Preposition
-----
Preposition Hit     :      0

Bytes Served
-----
Total Server Bytes:   :587112
Local Disk Reads     :      2
HTTP Based Reads     :      1
Bytes From Local Disk: 587112
Bytes Through HTTP:   293556

Rules
-----
Action Allow         :      0
Action Block         :      0
Validate url Sign    :      0
Errors               :      0
Auth Server Allow    :      0
Auth Server Deny     :      0

Error
-----
Invalid Error        :      0
Server Error         :      0
Media Not Found      :      0
Media Unauthorized   :      0
Invalid Request      :      0

```

- Step 5** To verify that the content has been cached after it was requested, enter the **show cache content** command.

```
NE-DEMO-SE2# show cache content
Max-cached-entries is set as 3000000
Number of cal cached assets: 1
-----
Priority          Size      URL
-----
1.71425e-01      293556   http://ofqdn.cds.com/vod-ecds/test_cache.flv
```

Verifying Flash Media Streaming—Live Streaming

Flash Media Streaming uses RTMP to stream live content by dynamic proxy. Configuration of live or rebroadcast programs is not required. When the first client requests live streaming content, the stream is created. There are no limits to the number of live streams other than the system load. Live streaming uses distributed content routing to distribute streams across multiple Service Engines.

- Step 1** Set up a Flash Media encoder. Enter the following information:
- FMS URL—Origin Server URL (Origin Server cannot be an ECDS device.)
 - Stream—Stream name for the client's request
 - Video—Choose VP6 or H.264
- Step 2** Click **Start** to publish the stream to the Origin Server.
- Step 3** In a web browser on the client PC, enter the URL `rtmp://<edge SE IP address>/live/<publish stream name>`.
- For example, if the URL was `rtmp://Temp4.se.fmslive.com/live/livestream`, *Temp4* is the SE assigned under the delivery service, the *live* directory indicates that it is a live stream, and *livestream* is the published name on the Flash Media Encoder.
- Step 4** On the Edge SE enter the **show statistics flash-media-streaming** command to view the Flash Media Streaming statistics.

```
NE-DEMO-SE2# show statistics flash-media-streaming
Flash Media Streaming Statistics
Statistics were last cleared on Thursday, 06-Dec-2011 37:22:58 UTC.
```

```
Connections
-----
Current          : 1
Current VOD      : 0
Current LIVE     : 1
Max Concurrent   : 1
Total            : 3
Total VOD Req    : 0
Total LIVE Req   : 0
Total DVRCast Req : 0
Total Other Proxy Req : 0

Live Streaming
-----
UpStream BW      : 0 kbps
DownStream BW    : 274 kbps
UpStream Bytes   : 3194
```

```
DownStream Bytes      : 124362967
Num of Instance Load : 1
```

Step 5 Enter the **show flash-media-streaming stream-status live** command.

```
NE-DEMO-SE2# show flash-media-streaming stream-status live
Display flash-media-streaming livestreams
```

Display maximum 4 applications, 8 forwarders, and 8 client stream info

```
Forwarder
-----
ClientReqUrl      : rtmp://Temp4.se.fmslive.com/live/livestream
path2OS           : 2.225.2.65->2.225.2.62
reqFwdUrl         : rtmp://2.225.2.65/live/cds_fms_proxy/2.225.2.62/live/livestream
Upstream BW (Kbps) : 0
Downstream BW (Kbps) : 267
Upstream Bytes    : 3487
Downstream Bytes  : 138278573
numClient         : 1
```

Step 6 On the Content Acquirer in the delivery service, enter the **show statistics flash-media-streaming** command. The command shows one session connecting from the edge SE.

```
NE-DEMO-SE2# show statistics flash-media-streaming
Flash Media Streaming Statistics
Statistics were last cleared on Thursday. 06-Dec-2011 37:22:58 UTC.
```

```
Connections
-----
Current          : 1
Current VOD      : 0
Current LIVE     : 1
Max Concurrent   : 1
Total            : 1
Total VOD Req    : 0
Total LIVE Req   : 0
Total DVRCast Req : 0
Total Other Proxy Req : 0
```

```
Live Streaming
-----
UpStream BW      : 0 kbps
DownStream BW    : 274 kbps
UpStream Bytes   : 3487
DownStream Bytes : 149456451
Num of Instance Load : 1
```

Step 7 Enter the **show flash-media-streaming stream-status live** command. The command shows the client request URL connecting from the edge SE.

```
NE-DEMO-SE2# show flash-media-streaming stream-status live
Display flash-media-streaming livestreams
```

Display maximum 4 applications, 8 forwarders, and 8 client stream info

```
Forwarder
-----
ClientReqUrl      : rtmp://2.225.2.65/live/cds_fms_proxy/2.225.2.62/live/livestream
path2OS           : 2.225.2.62
reqFwdUrl         : rtmp://2.225.2.62/live/livestream
Upstream BW (Kbps) : 0
Downstream BW (Kbps) : 261
Upstream Bytes    : 3337
```



```
Downstream Bytes      : 155736798  
numClient              : 1
```



APPENDIX **F**

Configuring Primary and Backup Proxy Servers

The following sections describe how to configure primary and backup (failover) proxy servers:

- [Configuring Primary Proxy Failover, page F-2](#)
- [Designating a Primary Outgoing HTTP Proxy Server, page F-3](#)
- [Designating a Primary Outgoing FTP Proxy Server, page F-3](#)
- [Designating a Primary Outgoing HTTPS Proxy Server, page F-4](#)
- [Configuring HTTP and HTTPS Outgoing Proxy Exclusion Settings, page F-5](#)
- [Monitoring Outgoing Proxy Servers and Statistics, page F-7](#)
- [Displaying the Current Outgoing Proxy Server Configuration, page F-8](#)
- [Displaying Outgoing Proxy Server Statistics, page F-8](#)



Note

For complete syntax and usage information for the CLI commands used in this chapter, see the [Cisco ECDS 2.5 Command Reference](#).

For information about configuring primary and backup proxy servers for Service Engines that are registered with a Content Distribution Manager, see the [Cisco ECDS 2.5 Software Configuration Guide](#).

Configuring Primary Proxy Failover

For HTTP proxy caching, there is a primary proxy failover option that you can configure on standalone Service Engines. This feature is referred to as the HTTP proxy failover feature. With this feature, you can configure the forward proxy server to contact up to eight other proxy servers (outgoing proxy servers) when an HTTP cache miss occurs (that is, when the requested HTTP content is not already stored locally in the Service Engine cache).

You can use the **http proxy outgoing** global configuration command to configure up to eight backup Service Engines or any standard proxy servers for the HTTP proxy failover feature. These outgoing proxy servers can be other Service Engines or standard proxy servers that can be contacted to process HTTP cache misses without using ICP or WCCP. The function of these outgoing proxy servers is to process the HTTP cache misses that have been forwarded to them by the forwarding proxy server. One outgoing proxy server functions as the primary server to receive and process all cache miss traffic.

If the primary outgoing proxy server fails to respond to the HTTP request, the server is noted as failed and the requests are redirected to the next outgoing proxy server until one of the proxies services the request.

Failover occurs in the order that the proxy servers were configured. If all of the configured proxy servers fail, the Service Engine can optionally redirect HTTP requests to the origin server specified in the HTTP header if you have used the **http proxy outgoing origin-server** global configuration command. If the **origin-server** option is not enabled, the client receives an error message. Response errors and read errors are returned to the client, because it is not possible to detect whether these errors are generated at the origin server or at the proxy.

**Note**

At any one time, the Service Engine uses only one of the configured outgoing proxy servers. They cannot be used simultaneously. The state of the outgoing HTTP proxy servers can be viewed in syslog NOTICE messages and with the **show http proxy EXEC** command.

By default, the Service Engine strips the hop-to-hop 407 (Proxy Authentication Required) error code sent by the Internet proxy. If you enter the **http proxy outgoing preserve-407** global configuration command on a standalone Service Engine, the Service Engine sends the 407 error code to the requesting client browser, and the Internet proxy authenticates the client.

Requests with a destination specified in the **proxy-protocols outgoing-proxy exclude** global configuration command bypass the primary outgoing proxy server and the failover proxy servers.

If all of the outgoing proxy servers fail to process the HTTP cache miss, the following occurs:

- If the **http proxy outgoing origin-server** option is enabled, then the Service Engine (forward proxy server) forwards the HTTP cache miss request to the origin server that was specified in the original HTTP request from the client browser.
- If the **http proxy outgoing origin-server** option is not enabled, an error is sent to the requesting client browser. Response errors and read errors are returned to the requesting client browser, because it is not possible to detect whether these errors are generated at the origin server or at the proxy server.

The **no http proxy outgoing connection-timeout** option causes the timeout to be set to the default value of 300 milliseconds.

In this example, the Service Engine is configured to redirect HTTP requests directly to the origin server if all of the proxy servers fail:

```
ServiceEngine(config)# http proxy outgoing origin-server
```

Requests with a destination specified in the **proxy-protocols outgoing-proxy exclude** global configuration command bypass the primary outgoing proxy and the failover proxy servers.

Designating a Primary Outgoing HTTP Proxy Server

To configure a standalone Service Engine to direct all HTTP miss traffic to a parent cache without using the Internet Cache Protocol (ICP) or WCCP, you must explicitly designate a proxy server as the primary outgoing HTTP proxy server for the Service Engine.

To designate a proxy server as the primary outgoing HTTP proxy server for the Service Engine, use the **http proxy outgoing host *host port* primary** global configuration command:

- *host* is the hostname or IP address of the outgoing HTTP proxy server.
- *port* is the port number designated by the outgoing (upstream) HTTP server to accept proxy requests.

To set the specified host as the primary outgoing HTTP proxy server, use the **primary** keyword. If several servers (hosts) are configured with the **primary** keyword, the last one configured becomes the primary outgoing HTTP proxy server for the Service Engine.

In this example, host 10.1.1.1 on port 8088 is explicitly designated as the primary outgoing HTTP proxy server for Service Engine A. Host 10.1.1.2 is configured as a backup outgoing HTTP proxy server.

```
ServiceEngineA(config)# http proxy outgoing host 10.1.1.1 8088 primary
ServiceEngineA(config)# http proxy outgoing host 10.1.1.2 220
```

Designating a Primary Outgoing FTP Proxy Server

You can configure up to eight proxy servers for FTP-over-HTTP missed traffic.



Note

At any one time, the Service Engine uses only one of the configured outgoing FTP-over-HTTP proxy servers. They cannot be used simultaneously.

To configure a standalone Service Engine to direct all FTP-over-HTTP miss traffic to a parent cache without using ICP or WCCP, you must explicitly designate the parent cache as the primary outgoing FTP-over-HTTP proxy server for the Service Engine.

To designate a proxy server as the primary outgoing FTP proxy server for the Service Engine, use the **ftp-over-http proxy outgoing host host port primary** global configuration command:

- *host* is the hostname or IP address of the parent cache (the outgoing FTP proxy server) to which FTP-over-HTTP missed traffic is directed.
- *port* is the port number used by the parent cache to accept missed FTP-over-HTTP requests from the Service Engine.

To set the specified host as the primary outgoing FTP proxy server, use the **primary** keyword. If several servers (hosts) are configured with the **primary** keyword, the last one configured becomes the primary outgoing FTP-over-HTTP proxy server for the Service Engine.

In this example, host 10.1.1.1 on port 8088 is explicitly designated as the primary outgoing FTP-over-HTTP proxy server for Service Engine A. Host 10.1.1.2 is configured as a backup outgoing FTP-over-HTTP proxy server:

```
ServiceEngineA(config)# ftp-over-http proxy outgoing host 10.1.1.1 8088 primary
ServiceEngineA(config)# ftp-over-http proxy outgoing host 10.1.1.2 220
```

Designating a Primary Outgoing HTTPS Proxy Server



Note

At any one time, the Service Engine uses only one of the configured outgoing HTTPS proxy servers; they cannot be used simultaneously.

To configure a standalone Service Engine to direct all HTTPS miss traffic (HTTPS-over-HTTP) to a parent cache without using ICP or WCCP, you must explicitly designate a proxy server as the primary outgoing HTTPS proxy server for the Service Engine.

To designate a proxy server as the primary outgoing HTTPS proxy server for the Service Engine, use the **https proxy outgoing port primary** global configuration command:

- *host* is the hostname or IP address of the parent cache (outgoing HTTPS proxy server) to which HTTPS missed traffic is directed.
- *port* is the port number used by the parent cache to accept missed HTTPS-over-HTTP requests from the Service Engine.

To set the specified host as the primary outgoing HTTPS proxy server, use the **primary** keyword.

If several servers (hosts) are configured with the **primary** keyword, the last one configured becomes the primary outgoing HTTPS proxy server for the Service Engine.

In this example, Service Engine A is configured to send its missed HTTPS traffic (that is, cache misses for browser requests for HTTPS content [HTTPS-over-HTTP requests]) to the host 10.1.1.1 on port 8088. Host 10.1.1.1 is explicitly designated as the primary outgoing HTTPS proxy server for Service Engine A. Host 10.1.1.2 is configured as a backup outgoing HTTPS proxy server for Service Engine A.

```
ServiceEngineA(config)# https proxy outgoing host 10.1.1.1 8088 primary
ServiceEngineA(config)# https proxy outgoing host 10.1.1.2 220
```

Configuring HTTP and HTTPS Outgoing Proxy Exclusion Settings

Some situations involve the deployment of a Service Engine in proxy mode at company headquarters and Service Engines in transparent mode at remote locations in branch offices. In this situation, if a cache miss occurs at the remote Service Engine, company policy requires that the request be routed to the Service Engine at headquarters.

When an HTTP request intended for another proxy server is intercepted by the Service Engine in transparent mode, the Service Engine forwards the request to the intended proxy server if the **proxy-protocols transparent original-proxy** global configuration command was entered. If this command was not entered, then the Service Engine forwards the request directly to the origin server.

When the Service Engine is operating in transparent mode, it can intercept requests that were sent to another proxy server and send these requests to one of the following two destinations:

- **Default server**—This is the default option. The Service Engine retrieves the objects from the origin server itself, or if it is configured to use an outgoing proxy server for this protocol, it forwards the request to the specified outgoing proxy server. In this situation, the client browser configuration is ignored, and the Service Engine configuration is used to retrieve the object from the server.
- **Original proxy**—The Service Engine forwards the request to the proxy server that the client originally addressed the request to. This may be different from the Service Engine's own outgoing proxy server for the specified protocol.

The ECDS software also has an option that allows you to specify a single domain name, hostname, or IP address to be globally excluded from proxy forwarding. The wildcard character * (asterisk) can be used for IP addresses (for instance, 172.16.*.*).



Note Requests with a destination specified with wildcard characters bypass the Service Engine proxy as well as the failover proxies.

The Service Engine addresses the request to the destination server directly and not to the client's intended proxy server.

When a Content Engine intercepts a proxy request intended for another proxy server and there is no outgoing proxy server configured for HTTPS-over-HTTP, and the **proxy-protocols transparent default-server** global configuration command is configured, the Service Engine addresses the request to the destination server directly and not to the client's intended proxy server.

However, all transparently intercepted requests sent by clients are returned to the client and requested objects are not delivered if the following two conditions exist:

- The **proxy-protocols transparent reset** command is configured on the Service Engine.
- A cache miss occurs.

You can use the Service Engine GUI or the CLI to configure HTTP and HTTPS outgoing proxy exclusion settings.

- From the Service Engine GUI, choose **Caching > Proxy Protocols**. Use the displayed Proxy Protocols window to configure these settings for this standalone Service Engine. For more information about how to use the Proxy Protocols window, click the **HELP** button in the window.
- From the Service Engine CLI, use the **proxy-protocols** global configuration commands. See [Table F-1](#) and [Table F-2](#). The order in which the CLI commands are entered is not important.

Table F-1 Proxy Protocols Key Parameters

Key Service Engine GUI Parameter	Description	Corresponding Service Engine CLI Command
Default server	Specifies that the Service Engine should retrieve objects from the origin server itself. With this option, a proxy-style request can be sent to an outgoing proxy server if such a server is configured.	proxy-protocols transparent default-server
Original Proxy	Specifies that the Service Engine should forward the request to the original proxy addressed in the client request.	proxy-protocols transparent original-proxy
Do not use Outgoing Proxy for the following domains	Excludes the domain name, hostname, or IP address specified here from proxy forwarding.	proxy-protocols outgoing proxy-exclude

To specify a domain name, hostname, or IP address to be excluded from proxy forwarding, use the **proxy-protocols** global configuration command. To selectively turn off outgoing-proxy exclude lists or to force transparently received proxy-style requests to be fulfilled by the Service Engine, use the **no** form of this command.

proxy-protocols outgoing-proxy exclude {enable | list word}

proxy-protocols transparent {default-server | original-proxy | reset}

[Table F-2](#) describes the parameters for the **proxy-protocols** command.

Table F-2 Parameters for the proxy-protocols Command

Parameter	Description
outgoing-proxy exclude	Sets global outgoing proxy exclude criteria.
enable	Enables global outgoing proxy exceptions.
list	Sets the global outgoing proxy exclude list.
<i>word</i>	Domain names, hostnames, or IP addresses to be excluded from proxy forwarding (supports 64 exclude list entries).
transparent	Sets transparent mode behavior for proxy requests.
default-server	Uses the Service Engine to go to the origin server or the outgoing proxy server, if configured.
original-proxy	Uses the intended proxy server from the original request.
reset	Resets the incoming connection.

The **proxy-protocols outgoing-proxy exclude** option allows you to specify a single domain name, hostname, or IP address to be globally excluded from proxy forwarding. For example, if you enter the domain name `cisco.com`, then the configured outgoing proxy server will be bypassed each time the Service Engine tries to retrieve a web page from `cisco.com`. You can specify IP addresses instead of domain names. The wildcard character (*) can also be specified for IP addresses (for instance, `174.12.*.*`). You must press the **Enter** key after entering each local domain.

Domains are entered as an ASCII string, separated by spaces. The wildcard character * (asterisk) can be used for IP addresses (for instance, `172.16.*.*`). Only one exclusion can be entered per command line. Enter successive command lines to specify multiple exclusions. Requests with a destination specified in the **proxy-protocols outgoing-proxy exclude** command bypass the Service Engine proxy as well as the failover proxy servers.

When you enter the **proxy-protocols transparent default-server** global configuration command, the Service Engine forwards intercepted HTTP, HTTPS-over-HTTP, and FTP-over-HTTP requests to the corresponding outgoing proxy server, if one is configured on the Service Engine. If no outgoing proxy server is configured for the protocol, the request is serviced by the Service Engine and the origin server.

The **proxy-protocols transparent original-proxy** option specifies that requests sent by a web client to another proxy server, but intercepted by the Service Engine in transparent mode, be directed back to the intended proxy server.

The **proxy-protocols transparent reset** option specifies that requests sent by a web client to another proxy server, but intercepted by the Service Engine in transparent mode, be returned to the web client during a cache miss. The requested objects are not delivered.

The following example configures the Service Engine to forward intercepted HTTPS-over-HTTP requests to an outgoing proxy server. The domain name `cruzio.com` is excluded from proxy forwarding.

```
ServiceEngine(config)# https proxy outgoing host 172.16.10.10 266
ServiceEngine(config)# proxy-protocols transparent default-server
ServiceEngine(config)# proxy-protocols outgoing-proxy exclude list cruzio.com
```

To verify the configuration, enter the **show proxy-protocols EXEC** command.

```
ServiceEngine# show proxy-protocols all
Transparent mode forwarding policies: default-server
Outgoing proxy exclude list is enabled
Outgoing exclude domain name: cruzio.com
```

The following example configures the Service Engine to forward intercepted HTTP proxy-style requests to the intended proxy server:

```
ServiceEngine(config)# proxy-protocols transparent original-proxy
```

Monitoring Outgoing Proxy Servers and Statistics

A background process on the Service Engine monitors the state of the configured outgoing proxy servers. You can configure the Service Engine to poll the specified outgoing proxy servers at a specific interval in order to monitor their availability.

This monitor interval is the frequency which the proxy servers are polled. The monitoring interval is specified in seconds, and can be from 10 to 300 seconds. The default monitoring interval is 60 seconds. If one of the outgoing proxy servers is unavailable, the polling mechanism waits for the connect timeout (300000 microseconds) before polling the next outgoing proxy server.

Use the following global configuration commands to specify the monitoring interval:

- To specify how frequently the Service Engine polls the specified outgoing HTTP proxy servers, use the **http proxy outgoing monitor** command.
- To specify how frequently the Service Engine polls the specified outgoing HTTPS proxy servers, use the **https proxy outgoing monitor** command.
- To specify how frequently the Service Engine polls the specified outgoing FTP proxy servers, use the **ftp-over-http proxy outgoing monitor** command.

In this example, the Service Engine is configured to monitor the outgoing HTTP proxy servers every 120 seconds:

```
ServiceEngine(config)# http proxy outgoing monitor 120
```

You can also monitor outgoing proxy servers by checking the syslog NOTICE messages on the Service Engine.

Displaying the Current Outgoing Proxy Server Configuration

To display the Service Engine's current outgoing proxy server configuration, use the following EXEC commands:

- To display the current outgoing HTTP proxy server configuration, enter the **show http proxy** command.
- To display the current outgoing HTTPS proxy server configuration, enter the **show https proxy** command.
- To display the current outgoing FTP-over-HTTP proxy server configuration, enter the **show ftp-over-http** command.

Displaying Outgoing Proxy Server Statistics

To display statistics about the HTTP requests that the Service Engine has sent to the specified HTTP proxy server, enter the **show statistics http proxy outgoing** EXEC command.

To display statistics about the FTP-over-HTTP requests that this Service Engine has sent to the specified FTP-over-HTTP proxy server, enter the **show statistics ftp-over-http** EXEC command.



Software Licensing Information

The following sections describe licensing information for Cisco ECDS software:

- [OpenSSL/Open SSL Project](#), page G-1
- [Open Source Used In Cisco Enterprise Content Delivery System 2.5.3](#), page G-3

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
 “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.
 The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Open Source Used In Cisco Enterprise Content Delivery System 2.5.3

This document contains the licenses and notices for open source software used in this product. With respect to the free/open source software listed in this document, if you have any questions or wish to receive a copy of the source code to which you are entitled under the applicable free/open source license(s) (such as the GNU Lesser/General Public License), please contact us at external-opensource-requests@cisco.com.

http://www.cisco.com/en/US/docs/video/ecds/2.5/open_source/osld_ecds_5.2.3.html



Unsupported Features

The following sections list features and functions that are not supported:

- [Unsupported in Cisco ECDS, page H-1](#)
- [Unsupported in Cisco ECDS with WCCP, page H-2](#)
- [Where to Go Next, page H-2](#)

Unsupported in Cisco ECDS

The following features may appear in the Enterprise CDSM interface but are not supported in the current release:

- DVRCAST
- ICAP
- IP-based Redirection
- IP multicast routing
- Geo-Location Server integration
- Proximity Server
- PCMM
- RTMPT
- RTMPTE
- Session Shifting
- Show and Share over SSL
- URL Signing
- Wholesale licensing
- Windows Media Services Multi Bit Rate

Unsupported in Cisco ECDS with WCCP

The following features may be supported by WCCP but are not supported on Cisco ECDS, the Service Engine, or other components of the system:

- Access Control Lists with WCCP
- Bypass Error handling
- Encrypted private keys for configuring the HTTPS server
- HTTPS without WCCP
- IP ACL
- IP multicast routing
- IP Spoofing with non-HTTP protocols or multiple Service Engines
- L4 Switch for the bypass gateway.
- Reverse proxy
- RTMP unmanaged domain
- Security proxy
- Show and Share over SSL
- WCCP CIF/FTP/DNS traffic caching
- WCCP Web cache packet return

Where to Go Next

For complete ECDS hardware and software support information, see the [Cisco ECDS 2.5 Release Notes](#) on Cisco.com.



INDEX

Symbols

- * wildcard character [F-7](#)
- <CdnManifest> tag [B-23](#)
- <contains> tag [B-45](#)
- <contentType> tag [B-25](#)
- <crawler> tag [B-37](#)
- <extension> tag [B-26](#)
- <host> tag [B-27](#)
- <item> tag [B-30](#)
- <item-group> tag [B-41](#)
- <match> subtag
 - time-before attribute
 - relative time [B-44](#)
- <matchRule> tag [B-43](#)
- <options> tag [B-26](#)
- <playServer> tag [B-24, B-25](#)
- <playServerTable> tag [B-24](#)
- <proxyServer> tag [B-29](#)
- <server> tag [B-27](#)

A

- access lists [10-15](#)
 - configuration, displaying [10-13](#)
- acquirer
 - delivery service information and content acquisition progress, displaying [10-13](#)
- acquisition content
 - specifying priority [B-10](#)
- admin password [3-2](#)
- alarms [10-2](#)
 - device reporting [10-2](#)

- displaying status and history [10-13](#)
- Apache CLF transaction logging format [10-43](#)
- Apple HTTP Live Streaming [5-15](#)
- ARP table, displaying [10-13](#)
- audit trail logs [10-6](#)
- authentication [1-10](#)
 - configuration, displaying [10-13](#)
 - login
 - RADIUS server [5-66](#)
 - TACACS+ server [5-66](#)
- Authorization Service configuration file [D-1](#)

B

- backup and restore
 - cms database [11-16](#)
- bandwidth
 - displaying [10-13](#)
- baseline groups [2-3](#)
- bit rate
 - displaying [10-13](#)
- bypass lists [5-42](#)

C

- cache content [10-13](#)
- cache-fill operations [1-9](#)
- cache miss [2-23](#)
- cache noncacheable settings [5-47](#)
- caching
 - HTTP
 - displaying [10-15](#)
- Cap-X profile ID [10-13](#)

- cdnfs
 - information, displaying [10-14](#)
- CdnManifest.xsd [B-46](#)
- CDSM redundancy [1-33](#)
- change report settings [10-24](#)
- Cisco Technical Assistance Center (TAC) [10-18](#)
- CLF
 - log file format [10-42](#)
- client IP spoofing [2-23](#)
- clock
 - system clock settings, displaying [10-14](#)
- CMS
 - process information, displaying [10-14](#)
- cms database
 - backup and restore procedure [11-16](#)
- command
 - service-router access-policy [1-28](#)
 - show statistics service-router summary [1-28](#)
- commands
 - acquirer start-delivery-service [B-13](#)
 - alarm nic-shutdown enable [5-96](#)
 - cdnfs browse [A-13](#)
 - cms database backup [11-16](#)
 - cms database delete [11-11](#)
 - cms database downgrade [11-5](#)
 - cms database restore [11-17](#)
 - cms deregister [11-11](#)
 - cms deregister force [3-13, 11-11](#)
 - cms enable [11-5, 11-11, 11-14](#)
 - cms recover identity [11-15, 11-19](#)
 - copy disk ftp [11-16](#)
 - debug acquirer trace [A-11](#)
 - debug ip wccp events [A-7](#)
 - debug ip wccp packets [A-7](#)
 - debug wccp [A-6](#)
 - debug wccp all [A-7](#)
 - disk reformat [11-20](#)
 - disk repair [11-20](#)
 - https server [5-48](#)
 - ip wccp redirect exclude in [7-21](#)
 - ip wccp redirect out [7-20](#)
 - no wccp [2-20](#)
 - show acquirer delivery-services [A-10](#)
 - show acquirer progress [A-10](#)
 - show cache content [E-5, E-22](#)
 - show distribution forwarder-list [2-5](#)
 - show distribution location
location-leader-preference [2-5](#)
 - show distribution object-status [A-12, E-1, E-20](#)
 - show distribution remote traceroute [A-9](#)
 - show flash-media-streaming stream-status live [E-26](#)
 - show ip wccp 80 detail [7-23](#)
 - show ip wccp detail [7-24](#)
 - show ip wccp web-cache detail [7-23](#)
 - show statistics acquirer delivery-service [A-11](#)
 - show statistics acquirer errors delivery-service [A-11](#)
 - show statistics flash-media-streaming [E-21](#)
 - show statistics http requests [E-2](#)
 - show statistics movie-streamer all [E-16](#)
 - show statistics service-router all [A-2](#)
 - show statistics wmt streamstat [E-9](#)
 - show wccp [A-4](#)
 - tcpdump [A-8](#)
 - verify https
 - show https server [5-48](#)
 - wccp flow-redirect [2-20](#)
 - wccp flow-redirect enable [2-20, 7-2](#)
 - wccp port-list [7-17](#)
 - wccp router-list-num [7-22](#)
 - wccp rtsp router-list-num [7-23](#)
 - wccp service-number [7-17, 7-24](#)
 - wccp shutdown max-wait [7-2, 7-3](#)
 - wccp slow-start enable [2-21, 7-2](#)
 - wccp web-cache mask src-ip-mask [7-23](#)
 - wccp web-cache router [7-22](#)
 - wccp web-cache router-list-num 1 mask-assign [7-23](#)
- Common Log Format. *See* CLF
- configuration

- IP Spoofing commands [7-20](#)
- configuring a Movie Streamer [8-27](#)
- configuring cross-domain policy [1-28](#)
- configuring Windows Media [8-27](#)
- content
 - mapping [B-24](#)
- Content Acquirer [2-4](#)
 - redundancy [1-32](#)
- content acquirer [1-7](#)
- content acquirer HTTP server [2-12](#)
- content acquirer SMB server [2-11](#)
- content acquisition
 - scheduling [B-7](#)
- content attributes
 - listing [B-30](#)
- content completeness [1-10](#)
- content freshness [1-9](#)
- Coordinated Universal Time. *See* UTC
- Coverage Zone [2-8](#)
- Coverage Zone file [C-1](#)
- coverage zone file [1-23](#)
- coverage zones
 - file elements [C-2, D-1](#)
- crawler attributes [B-4](#)
- crawler filter
 - specifying [B-8](#)
- crawler jobs [B-4](#)
- crawler tag
 - prefix attribute [B-6](#)
- crawl filter
 - example [B-8](#)
- crawl job
 - example [B-5](#)
 - prefix attribute example [B-6](#)
- cross-domain policy [1-27](#)
- custom transaction log format
 - description [10-43](#)

D

- database backup [11-16](#)
- debug command examples [A-6](#)
- defining a crawl task [8-13](#)
- deleting a device
 - before deleting [11-10](#)
- CLI
 - adding device back into the ECDS network [11-12](#)
 - remove and deregister a device [11-11](#)
- deleting warm standby ECDSM [11-13](#)
- Service Routers from network [11-10](#)
- using ECDSM [11-12](#)
- delivery service [2-3](#)
- delivery service distribution
 - information, displaying [10-14](#)
- delivery service methods [2-9](#)
- delivery services [2-9](#)
 - hybrid ingest [8-1](#)
 - live programs [8-1](#)
 - prefetch ingest [8-1](#)
- delivery services management [1-32](#)
- delivery traffic
 - view statistics [10-37](#)
- device alarms
 - description [10-2](#)
- device groups [2-3](#)
 - verifying devices
 - show config commands [4-6, A-3](#)
- device management [1-31](#)
- device mode
 - displaying [10-14](#)
- device registration information
 - recovering [11-18](#)
- device replication states [10-39](#)
- device security
 - activating a device [3-3](#)
- Devices home page [10-11](#)
- directing requests back to proxy server [F-7](#)

Direct Server Return (DSR)

information, displaying [10-14](#)

disks

details, viewing [10-14](#)

distribution

delivery service, displaying [10-14](#)

statistics

displaying [10-14](#)

troubleshooting [A-8](#)

distribution tree [2-8](#)

documentation, related [1-xxi](#)

dynamic WCCP redirection [2-17](#)

E

ECDSM database backup [11-16](#)

ECDS network

content type mapping [B-25](#)

ECDS program [2-27](#)

ECDS software recovery [11-16](#)

ECDS system home page [10-4](#)

edit a delivery service [8-4](#)

enable cache query string [5-47](#)

Enterprise Content Delivery System Manager [1-31](#)

entities

defined [9-6](#)

exporting

log files [10-45](#)

extended IP ACLs

ICMP message types [5-90](#)

TCP keywords [5-90](#)

Extended Squid transaction log format [10-43](#)

external FTP server

exporting transaction logs to [10-46](#)

permanent error from [10-46](#)

F

file attribute

marking for import [B-30](#)

file extension

mapping [B-24](#)

tag [B-26](#)

Flash Media

streaming [5-37](#)

Flash Media Streaming

information, displaying [10-14](#)

Flash Media Streaming Engine [1-16](#)

codecs [1-18](#)

flash media streaming proxy [1-18](#)

HTTP requests [1-16](#)

interactive applications [1-20](#)

live streaming [1-19](#)

multi-bit rate streaming [1-18](#)

RTMP requests [1-16](#)

unicast streaming [1-18](#)

flash memory

version and usage, displaying [10-14](#)

forwarding

HTTP, HTTPS, and FTP proxy-style requests [F-7](#)

ftp-over-http proxy outgoing monitor command [F-8](#)

ftp proxy outgoing host command [F-4](#)

FTP servers

exporting transaction logs to [10-46](#)

G

global exclusion from proxy forwarding [F-7](#)

GMT offsets [B-52 to B-61](#)

Africa [B-54](#)

America [B-55](#)

Antarctica/Arctic [B-56](#)

Asia [B-56](#)

Atlantic [B-57](#)

Australia [B-57](#)

Brazil [B-58](#)
 Canada/Chile [B-58](#)
 Egypt/Europe [B-58](#)
 Hong Kong/Iceland/India/Iran/Israel [B-59](#)
 Jamaica/Japan/Kwajalein/Libya [B-59](#)
 Mexico/Mideast [B-60](#)
 Pacific/Poland/Portugal [B-60](#)
 Singapore/System V/Turkey [B-60](#)
 U.S. [B-61](#)
See also UTC offsets

guide

conventions [1-xx](#)

H

hardware clock [5-79](#)

hardware interface

displaying information [10-15](#)

hardware status, displaying [10-15](#)

hierarchical caching proxy [1-11, 1-15](#)

hosts

name servers and IP addresses, displaying [10-15](#)

HTTP

configuring [5-39](#)

outgoing proxy exclusion [F-5](#)

proxy failover [F-2](#)

HTTP connections [2-7](#)

http connections fields

acquirer outgoing proxy authentication [5-40](#)

enable incoming proxy [5-40](#)

enable IP spoofing [5-40](#)

enable outgoing proxy [5-40](#)

list of incoming http ports [5-40](#)

maximum concurrent connections [5-40](#)

outgoing http proxy bypass domains [5-41](#)

outgoing http proxy bypass list [5-41](#)

outgoing proxy [5-40](#)

HTTP download

disabling [2-12](#)

http proxy outgoing host command [F-3](#)

http proxy outgoing monitor command [F-8](#)

http proxy outgoing origin-server command [F-2](#)

HTTPS

filtering servers [5-63](#)

transparent caching

SSL [2-24](#)

https

configuring

importing self-signed certificates and keys [5-48](#)

HTTPS caching [2-24](#)

HTTPS certificate groups [5-54](#)

create new [5-55](#)

filtering [5-56](#)

HTTPS certificates [2-25](#)

create new [5-49](#)

HTTPS configuration

CLI config examples [5-63](#)

https debugging [5-64](#)

https for wccp

configuring [5-48](#)

HTTPS keys [5-57](#)

create new [5-57](#)

filtering [5-59](#)

HTTPS outgoing proxy servers

displaying current state of [A-5](#)

https proxy outgoing host command [F-4](#)

https proxy outgoing monitor command [F-8](#)

HTTPS redirection [2-24](#)

HTTPS server

create new [5-61](#)

HTTPS servers

configuring [5-60](#)

https statistics [5-64](#)

ICMP

keywords for message type and code [5-90](#)

icons

- ECDS task bar [3-9](#)
- service control [5-11](#)
- service engine assignment [5-5](#)
- service engine replication bandwidth [5-6](#)

implicit URI [1-20](#)incoming bandwidth bypass [5-31](#)

ingest

- preparing Movie Streamer content [E-11](#)

interface

- displaying hardware status [10-15](#)
- standby [10-17](#)

inventory information

- displaying [10-15](#)

IP ACL

- adding conditions to [5-86](#)
- applying to interface [5-92](#)
- CLI [5-92](#)
- configuration constraints [5-85](#)
- creating new [5-85](#)
- deleting [5-93](#)

K

- keepExpiredContent attribute [B-39](#)
- keepNoCacheContent attribute [B-39](#)
- keepQueryUrl attribute [B-39](#)
- kernal debugger
 - enabling [A-13](#)

L

- last-resort routing [6-4](#)
- licensing information [G-1](#)
- live delivery service [2-9](#)
- live events [2-27](#)
- Live stream interruptions [8-26](#)
- live stream splitting

Flash Media Streaming Engine [1-8](#)Movie Streamer Engine [1-8](#)Windows Media Engine [1-8](#)

load balancing hash

HTTPS default hashing target

source IP [7-7](#)location leader [2-5](#)

locations

Location Tree [2-3](#)

log fields

Flash Media Streaming [10-56](#)Movie Streamer [10-54](#)Windows Media Streaming [10-48](#)

log files

- exporting [10-45](#)
- restarting export of [10-46](#)

log formats

- custom transaction log string values [10-43](#)
- Windows Media Services Version 9.0 [10-48](#)
- WMT transaction logging [10-47](#)

logging formats [10-47](#)

login authentication

- about [9-1](#)

logs

- archives [10-45](#)
- directories [10-44](#)
- exporting [10-45](#)
- exporting to SFTP [10-46](#)
- filename formatting [10-45](#)
- Flash Media event types [10-62](#)
- Flash Media status codes [10-60](#)
- manage exporting of [10-45](#)
- permanent error response [10-46](#)
- SE transaction [10-63](#)

lost administrator passwords

- recovering [11-17](#)

M

- manifest file [2-10](#)
 - content serving [B-12](#)
 - samples [B-2](#)
 - single content example [B-3](#)
 - time strings
 - example [B-13](#)
- manifest file, crawling [2-11](#)
- manifest files [B-1](#)
 - hybrid ingest content example [B-15](#)
 - regular expressions [B-7](#)
 - requirements [B-2](#)
 - schema [B-46](#)
 - shared attributes example [B-8](#)
 - single content tags [B-3](#)
 - structure and syntax [B-19](#)
 - correcting [B-19](#)
 - tags (listing) [B-20](#)
 - time zones [B-52](#)
 - ttl attribute
 - refreshing and removing content [B-13](#)
 - Windows Media live content [B-14](#)
- manifest file syntax validator [B-15](#)
- manifest file validator
 - accessing [B-16](#)
 - output errors [B-18](#)
 - output examples [B-16](#)
- manifest tags
 - summary (table) [B-20](#)
- manifest XML schema [B-46](#)
- match subtag
 - attributes [B-9](#)
- MDE initial configuration [3-1](#)
- media attribute
 - marking for import [B-30](#)
- Media Streamer
 - redundancy [1-33](#)
- media streamer [1-8, 2-12](#)
- messages
 - here I am [2-16](#)
 - I see you [2-16](#)
- mibs
 - cisco-config-man-mib [5-107](#)
 - cisco-entity-asset-mib [5-107](#)
- MIBs, downloading [5-107](#)
- MIME content types [B-24, B-25](#)
- monitoring
 - alarms [10-1](#)
 - delivery service devices [10-31](#)
 - delivery service replication status [10-30](#)
 - delivery services [10-27](#)
 - delivery service states [10-30](#)
 - status errors
 - status lights [10-29](#)
 - system status [10-1](#)
 - System Status bar [10-1](#)
- Movie Streamer
 - configuration, displaying [10-15](#)
 - general settings [5-35](#)
- Movie Streamer Engine [1-14](#)
 - live stream [1-15](#)
 - transport types [1-15](#)
- multicast cloud, displaying information [10-14](#)

N

- network partitions [2-8](#)
- NIC alarm reporting [5-96](#)
- NTLM
 - authentication [10-44](#)
- NTP
 - and system clock [5-79](#)
 - status, displaying [10-16](#)
- NTP server [3-3](#)

O

origin server [2-10](#)
 origin server by proxy [2-10](#)
 outgoing FTP-over-HTTP proxy servers
 monitoring [F-8](#)
 outgoing FTP proxy servers
 configuration of [F-8](#)
 configuring [F-4](#)
 outgoing HTTP proxy servers [F-8](#)
 designating primary server [F-3](#)
 monitoring [F-7](#)
 outgoing HTTPS proxy servers
 configuration of [F-8](#)
 configuring [F-4](#)
 designating primary server [F-4](#)
 monitoring [F-8](#)
 outgoing proxy servers
 primary outgoing HTTP proxy server [F-3](#)
 overload bypass [2-21](#)

P

packet flow
 diagram [1-30](#)
 passwords
 administrator
 recovering [11-17](#)
 playserver list [B-11](#)
 example [B-11](#)
 playserver lists
 generating [B-11](#)
 playservers
 mappings
 accepted locations [B-24](#)
 settings
 versus <playServer> tag [B-25](#)
 PlayServerTable.xsd [B-51](#)
 playserver tables

 http playserver [B-11](#)
 PlayServerTable schema [B-51](#)
 policies
 and Rules Template [5-11](#)
 port lists
 configuring for WCCP [7-15](#)
 ports used by the ECDS [10-7](#)
 prefetch/caching delivery services [2-9](#)
 pre-positioning
 software files [11-2](#)
 primary outgoing proxy servers
 designating for FTP-over-HTTP [F-4](#)
 designating for HTTP [F-3](#)
 designating for HTTPS-over-HTTP [F-4](#)
 processes
 CPU or memory, displaying [10-16](#)
 programs
 displaying [10-16](#)
 modifying API-defined [8-38](#)
 previewing [8-39](#)
 viewing [8-37](#)
 provisioning the Cisco ECDS [2-1](#)
 proxy failover [F-2](#)
 proxy forwarding
 excluding items [F-6](#)
 proxy protocols
 parameters [F-6](#)
 proxy-protocols command [F-6](#)

Q

QoS
 managing with CLI [8-6](#)
 QoS settings [8-6](#)
 QoS unicast data [8-6](#)

R

RADIUS server
 information, displaying [10-16](#)
 rate of data transfer [1-10](#)
 reboot a device [11-9](#)
 reboot device group [11-9](#)
 rebooting
 Service Engines [11-9](#)
 reboot option
 Service Engines [11-9](#)
 rebroadcasts [2-27](#)
 recovering
 device registration information [11-18](#)
 lost administrator passwords [11-17](#)
 recover lost registration information [11-18](#)
 regular expressions
 writing [B-7](#)
 remote execution agent (REA) [10-16](#)
 replace a device [11-13](#)
 replace a failed node [11-18](#)
 replacing a disk [11-20](#)
 replacing an SE or SR [11-14](#)
 reportBrokenLinks attribute [B-40](#)
 reportes
 locations [10-23](#)
 reports
 bandwidth efficiency gain [10-25](#)
 bandwidth served [10-24](#)
 service engine [10-23](#)
 streaming sessions [10-26](#)
 system wide [10-23](#)
 request redirection [1-27](#)
 Request Routing Engine [1-21](#)
 routing redirection [1-21](#)
 request routing methods [1-24](#)
 resetting passwords
 bootflags [11-17](#)
 restarting export of log files [10-46](#)

RFQDN redirection [1-21](#)
 root location
 deleting Service Engines from [11-10](#)
 router
 commands, list of [7-21](#)
 configuring
 for web cache service [7-25, 7-27](#)
 enabling WCCP support [7-21](#)
 router lists
 configuring for WCCP [7-12](#)
 routing methods
 content-based [1-26](#)
 last resort [1-24](#)
 load-based [1-24](#)
 location-based [1-25](#)
 service aware [1-25](#)
 routing redirection [1-21](#)
 RFQDN redirection [1-21](#)
 RTMP and RTMPE streaming [5-37](#)
 RTSP
 configurations and license agreements [10-16](#)
 rules
 configuration, displaying [10-16](#)
 Rules Template
 actions
 order of execution [5-17](#)
 running configuration
 current profile, displaying [10-16](#)

S

sanitized transaction logs [10-45](#)
 search string characters [10-33](#)
 service alarms [10-3](#)
 Service Engine [1-7, 2-6](#)
 service engine coverage zone [1-23](#)
 Service Engines
 configuring
 for web cache services (scenarios) [7-25, 7-27](#)

- rebooting [11-9](#)
- restarting [11-9](#)
- upgrading software [11-5](#)
- service masks
 - configuring for WCCP [7-9](#)
- Service Router
 - redundancy [1-33](#)
- Service Routers
 - configuration [10-16](#)
 - troubleshooting configurations [A-2](#)
- service rules [1-10](#)
- services
 - information [10-16](#)
- service workflow [2-13](#)
- SFTP servers
 - exporting transaction logs to [10-46](#)
- shared attributes
 - specifying [B-7](#)
- show/clear command tool [10-12](#)
- show command examples [10-20](#)
- show ftp proxy command [F-8](#)
- show http proxy command [F-2, F-8](#)
- show https proxy command [F-8](#)
- show statistics http command [F-8](#)
- slow start caching service [7-2](#)
- SNMP
 - communications status, displaying [10-17](#)
- software
 - upgrading [11-1](#)
- software clock [5-79](#)
- software files
 - pre-positioning [11-2](#)
- SSH
 - configuration and status, displaying [10-17](#)
- SSL
 - caching HTTPS [2-24](#)
- standby interface
 - displaying information [10-17](#)
- startup configuration

- displaying [10-17](#)
- static caching proxy [1-11, 1-15](#)
- statistics for [F-8](#)
- syslog
 - configuration, displaying [10-15](#)
- system file system (sysfs) volumes [11-20](#)
- system hardware
 - displaying status [10-15](#)
- system inventory
 - displaying [10-15](#)
- system statistics [10-17](#)
- system status
 - monitoring [10-1](#)
- system status bar
 - troubleshooting
 - content replication [10-3](#)
 - devices [10-3](#)

T

- TAC
 - viewing technical support information [10-18](#)
- tags
 - in manifest files [B-20](#)
- TCP
 - keywords and port numbers [5-90](#)
- TCP flow [2-20](#)
- technical support information
 - viewing [10-18](#)
- Telnet services
 - configuration, displaying [10-18](#)
- time-to-live (TTL) [1-9](#)
- time zones
 - in manifest files [B-52](#)
- token strings
 - in custom transaction logging format [10-43](#)
- transaction logging
 - and NTLM authentication [10-44](#)
 - configuration and archived files, displaying [10-19](#)

- formats
 - W3C customizable [10-44](#)
- sanitized [10-45](#)
- WMT
 - about using [10-47](#)
 - log formats [10-47](#)
- transaction logs [10-41](#)
 - custom formats [10-43](#)
 - extended squid [10-42](#)
- transparent caching
 - and SSL [2-24](#)
 - outgoing proxy exclusion and [F-5](#)
- transparent interception
 - using WCCP [1-6](#)
- transparently received proxy-style requests [F-6](#)
- troubleshooting
 - acquisition [A-10](#)
 - content prefetched on a Service Engine [A-3](#)
 - devices in device groups [A-3](#)
 - distribution hierarchy [A-8](#)
 - DNS delegation [A-2](#)
 - kernel debugger [A-14](#)
 - Service Router configurations [A-2](#)
 - Service Router routing properties [A-2](#)
- ttl scheduling
 - example [B-7](#)

U

- UDP
 - keywords and port numbers [5-90](#)
- unsupported features [H-1](#)
- update software [11-5](#)
- upgrading software
 - determining software version [11-9](#)
 - interoperability considerations [11-6](#)
 - multiple Service Engines [11-7](#)
 - recommended order [11-6](#)
 - single device [11-8](#)

- tips [11-5](#)
- view progress [11-7](#)
- upgrading system software [11-5](#)
- URL signature
 - information, displaying [10-19](#)
- user accounts
 - managing [?? to 9-7](#)
- user authentication. *See* login authentication
- users
 - administrative and authenticated, displaying [10-19](#)
 - user identification number and name, displaying [10-19](#)
- UTC [5-79](#)
- UTC offsets [5-81](#)
 - See also* GMT offsets

V

- verifying
 - dynamically ingested Movie Streamer content [E-16](#)
 - dynamically ingested web content [E-3](#)
 - dynamically ingested Windows media content [E-8](#)
 - Flash Media Streaming, live streaming [E-25](#)
 - Flash Media Streaming dynamically ingested content [E-22](#)
 - Flash Media Streaming preingested content [E-20](#)
 - Movie Streamer live content playback [E-17](#)
 - preingested Movie Streamer content [E-13](#)
 - preingested web content [E-1](#)
 - preingested Windows media content [E-7](#)
 - Windows media live content playback [E-10](#)

- version
 - displaying information about [10-19](#)

W

- W3C customizable logging format [10-44](#)
- WCCP
 - clean shutdown

- description [2-20](#)
- client IP spoofing
 - description [2-23](#)
- configuring
 - general settings for the Service Engine [7-1](#)
 - port lists [7-15](#)
 - router lists [7-12](#)
 - service masks [7-9](#)
 - service settings for the Service Engine [7-3](#)
- custom web cache service [2-17](#)
- dynamic redirection services [2-17](#)
- dynamic service settings [7-6](#)
- enabling on router [7-21](#)
- information, displaying [10-19](#)
- IP ACL feature usage [5-93](#)
- load balancing [2-18](#)
- load balancing hash [7-6](#)
- packet flow diagram [1-30](#)
- service groups [2-16](#)
- source, destination IP hash [2-18](#)
- traffic bypass
 - viewing lists [7-19](#)
- transparent caching options [2-21, 7-18](#)
- wccp
 - redirect access list (ACL) settings [7-21](#)
- WCCP bypass
 - viewing lists [7-19](#)
- wccp configuration example
 - service engine, different subnets [7-29](#)
 - service engine, same subnet [7-26](#)
 - wccp-enabled router, different subnets [7-29](#)
 - wccp-enabled router, same subnet [7-26](#)
- WCCP general settings
 - command map [7-2](#)
- WCCP support
 - enabling on the router [7-21](#)
- WCCP transparent interception [1-6](#)
- web cache service
 - clients and cache on different subnets [7-27](#)
 - clients and cache on the same subnet [7-25](#)
 - configuration examples
 - for different subnets [7-29](#)
 - for same subnet [7-26](#)
- web engine [1-8](#)
- wildcard character * [F-7](#)
- windows media
 - outgoing proxy bypass list [5-32](#)
 - proxy bypass commands [5-32](#)
 - RTSP proxy bypass commands [5-34](#)
 - RTSP proxy bypass list [5-33](#)
- Windows Media Engine [1-10](#)
 - authentication [1-13](#)
 - bandwidth management [1-13](#)
 - fast cache [1-11](#)
 - fast start [1-11](#)
 - fast stream start [1-12](#)
 - multicast out [1-12](#)
 - policy server integration [1-14](#)
 - unicast out [1-13](#)
- windows media streaming [5-25](#)
- Windows Media Streaming Silverlight [1-27](#)
- WMT
 - configuration and license information, displaying [10-19](#)
 - Live Source URL, configuring [8-29](#)
- WMT transaction logging
 - about [10-47](#)
 - log formats [10-47](#)

X

- XML schema
 - manifest [B-46](#)
 - PlayServerTable [B-51](#)
- XSD [B-46](#)

Z

zero-ip based configuration [C-2](#)

