



## **Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Software Configuration Guide**

August 15, 2014

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide.  
Addresses, phone numbers, and fax numbers  
are listed on the Cisco website at  
[www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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](http://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 Videoscope Distribution Suite, Internet Streamer 4.0 Software Configuration Guide*

© 2014 Cisco Systems, Inc. All rights reserved.



## Preface xvii

Document Revision History	xvii
Audience	xvii
Objective	xvii
Document Organization	xviii
Document Conventions	xix
Related Documentation	xx
Obtaining Documentation and Submitting a Service Request	xxi

---

## CHAPTER 1

### Product Overview 1-1

Overview	1-1
Ingest and Distribution	1-3
Prefetch Ingest	1-3
Dynamic Ingest	1-3
Hybrid Ingest	1-4
Live Stream Ingest and Split	1-4
Delivery	1-4
Management	1-5
Content Delivery System Architecture	1-5
Service Engine	1-6
Storage and Distribution	1-6
Stream and Cache-Fill Performance	1-13
NAS	1-15
Content Acquirer	1-16
Internet Streamer	1-16
Service Router	1-34
Request Routing Engine	1-34
Proximity Engine	1-47
Content Delivery System Manager	1-51
Authentication, Authorization, and Accounting	1-51
Device Management	1-51
Delivery Services Management	1-52
Resiliency and Redundancy	1-52
Content Acquirer Redundancy	1-52

Internet Streamer Redundancy	1-53
Service Router Redundancy	1-53
Internet Streaming CDSM Redundancy	1-53

---

CHAPTER 2

**Network Design** 2-1

VDS-IS Topology	2-1
Device Groups	2-2
Baseline Groups	2-3
Delivery Service	2-3
Content Acquirer	2-3
Content Acquirer Selection for Prefetched Content	2-4
Content Acquirer Selection for Dynamic or Hybrid Ingest	2-4
Location Leader	2-5
Location Leader Selection for Prefetched Content	2-5
Location Leader Selection for Live Streaming	2-5
Location Leader Selection for Dynamic or Hybrid Content	2-5
Forwarder and Receiver Service Engines	2-5
Persistent HTTP Connections	2-7
Network Partition	2-7
Delivery Service Distribution Tree	2-8
Types of Delivery Services	2-8
Methods for Ingesting Content	2-9
Origin Servers	2-9
Manifest File	2-10
Content Acquirer	2-11
Internet Streamer	2-11
Content Replication Using a Multicast Cloud	2-12
Introduction to Multicast Cloud	2-12
Distributing Content Through Replication	2-13
Unicast Replication	2-13
Multicast Replication	2-13
Configuring Multicast Distribution	2-14
Multicast Forward Error Correction and Proactive Forward Error Correction	2-15
Configuring PGM and File Transmission Parameters Using Multicast Expert Mode	2-15
APIs for Multicast Cloud	2-18
Service Workflow	2-18
Programs	2-20
Live Programs	2-20
Rebroadcasts	2-21

API Program File	<b>2-21</b>
IPv6 Support for Client Interfaces	<b>2-21</b>
HTTPS Settings	<b>2-25</b>
Certificates	<b>2-25</b>
Traffic Separation for HTTPS	<b>2-26</b>
Configuring HTTPS	<b>2-28</b>
API Support for HTTPS	<b>2-30</b>
Wholesale CDN	<b>2-30</b>
Session and Bandwidth Quotas per Delivery Service	<b>2-30</b>
Monitoring Session and Bandwidth Quotas	<b>2-31</b>
Cache Storage Priority per Delivery Service	<b>2-32</b>
Snapshot Counters	<b>2-32</b>
Real-Time Exporting of Transaction Logs for Billing and Analytic Reports	<b>2-32</b>
APIs for Wholesale CDN	<b>2-32</b>

---

**CHAPTER 3****Getting Started** **3-1**

Initially Configuring the Devices	<b>3-1</b>
Logging In to the Internet Streaming CDSM	<b>3-1</b>
Activating and Synchronizing the Devices	<b>3-3</b>
Activating and Setting NTP for Each Device	<b>3-3</b>
Activating All Inactive Service Engines	<b>3-5</b>
Navigating the Internet Streaming CDSM	<b>3-7</b>
Devices, Services, and Other Tables	<b>3-7</b>
Devices Home Page	<b>3-8</b>
Task Bar	<b>3-9</b>
Configuring Primary and Standby CDSMs	<b>3-11</b>
Changing a Standby CDSM to a Primary CDSM	<b>3-12</b>
Recovering from two Primary CDSMs	<b>3-13</b>
Typical Configuration Workflow	<b>3-13</b>

---

**CHAPTER 4****Configuring Devices** **4-1**

Configuring Locations	<b>4-1</b>
Configuring Device Groups	<b>4-4</b>
Working with Device Groups	<b>4-6</b>
Aggregate Settings	<b>4-8</b>
Device Group Overlap	<b>4-9</b>
Configuring the Service Engine	<b>4-9</b>
Activating a Service Engine	<b>4-10</b>

Assigning Devices to Device Groups	4-14
Replication	4-15
Default Bandwidth	4-16
Scheduled Bandwidth	4-18
Configuring the NACK Interval Multiplier	4-20
Enabling SEs for Multicasting	4-20
Service Control	4-21
Configuring Service Rules	4-21
Configuring URL Signing Key	4-27
Configuring the Authorization Service	4-28
Configuring Transaction Logs	4-30
Application Control	4-34
Configuring Default and Maximum Bandwidth	4-34
Configuring Bandwidth Schedules	4-36
Configuring Windows Media Streaming—General Settings	4-38
Configuring Windows Media Streaming—Bypass List	4-40
Configuring Movie Streamer—General Settings	4-41
Configuring RTSP Advanced Settings	4-43
Configuring Flash Media Streaming—General Settings	4-43
Configuring Flash Media Streaming—FMS Administrator	4-44
Configuring Flash Media Streaming—Service Monitoring	4-44
Configuring Web Engine HTTP Cache Freshness	4-45
Configuring Tmpfs Size Settings	4-46
General Settings	4-46
Configuring Content Management	4-47
Login Access Control	4-49
Authentication	4-56
Scheduling Database Maintenance	4-60
Setting Storage Handling	4-61
Network Settings	4-63
Configuring Notification and Tracking	4-81
Configuring Troubleshooting	4-97
Configuring Service Router Settings	4-98
Configuring Cache Router Settings	4-98
Configuring Memory Limitation Settings	4-99
Configuring the Service Router	4-99
Activating a Service Router	4-100
Configuring Routing Settings	4-104
Configuring Request Routing Settings	4-104
Configuring IP-based Redirection	4-109

**CHAPTER 5**

Configuring DNS-based Redirection	4-109
Configuring Redirect Burst Control	4-110
Configuring Cross-Domain Policy	4-110
Configuring the Proximity Server Settings	4-111
Configuring Application Control	4-122
Configuring Load Monitoring	4-122
Configuring Last-Resort Routing	4-124
Creating ASX Error Message Files for Windows Media Live Programs	4-127
Configuring Domain Subscription	4-128
Configuring Memory Limitation Settings	4-128
Configuring Transaction Logs for the Service Router	4-129
Configuring the CDSM	4-131

**Configuring Services 5-1**

Configuring Delivery Services	5-1
Content Origins	5-1
Creating Multicast Clouds	5-8
Assigning SEs to a Multicast Cloud	5-12
Assigning Multicast Clouds to Delivery Services	5-14
Creating Storage Priority Classes	5-15
Creating Delivery Service	5-16
Identifying Content	5-33
Identifying Content Using the CDSM	5-33
Identifying Content Using a Manifest File	5-43
Verifying Content Acquisition	5-47
Configuring Programs	5-47
Defining a Program	5-48
Configuring Live Programs	5-49
Priming a Live Delivery Service	5-54
Windows Media Streaming Live Streaming Encoder Failover	5-54
Configuring a Rebroadcast	5-55
Viewing the Multicast Addresses	5-59
Viewing Programs	5-59
Viewing and Modifying API Programs	5-61
Previewing a Program	5-62
Copying a Program	5-62

**CHAPTER 6****Configuring the System 6-1**

Configuring AAA	6-1
-----------------	-----

Creating, Editing, and Deleting Users	6-2
Creating, Editing, and Deleting Roles	6-5
Creating, Editing, and Deleting Domains	6-6
Viewing Locked Users	6-7
Changing a Password	6-7
Configuring System Settings	6-8
System Properties	6-8
Configuring Device Offline Detection	6-10
Configuring Distribution QoS	6-10
Configuring Service Routing	6-12
Coverage Zone File Registration	6-12
Configuring Global Routing	6-14
Authorization File Registration	6-15
NAS File Registration	6-16
HTTPS Settings	6-17
Configuring HTTPS General Settings	6-18
Uploading or Importing a Root CA File	6-18
Uploading a CRL File	6-19
Scheduling a CRL File	6-20
Uploading Certificate and Key Files	6-21
Scheduling Web Engine Notification of Certificate and Key Files	6-22
Configuring the CDSM to Communicate with an External System	6-23
Viewing or Downloading XML Schema Files	6-24

---

CHAPTER 7

**Configuring Licenses** 7-1

Viewing CDN License Summary	7-2
Configuring License Files	7-3
Purchase Information	7-3
License Logs	7-4

---

CHAPTER 8

**Monitoring the Videoscape Distribution Suite, Internet Streamer** 8-1

System Monitoring	8-1
System Status	8-1
Device Alarms	8-4
Service Alarms	8-5
License Alarms	8-6
System Home Page	8-7
System Audit Logs	8-9
System Port Numbers	8-10

Device Monitoring	8-13
Devices Table	8-13
Devices Home Page	8-15
Using show and clear Commands	8-17
Using the CDSM show or clear Command Tool	8-17
Core Dump Files	8-24
CPU Utilization	8-25
Reports	8-26
Bandwidth Served	8-27
Bandwidth Efficiency Gain	8-28
Streaming Sessions	8-29
Delivery Service Monitoring	8-30
Delivery Services Table	8-30
Processing Content Deletion	8-34
Content Deletion Tasks	8-35
Replication Status for a Delivery Service	8-37
Content Replication Status by Delivery Service	8-40
Content Replication Status by Device	8-42
Viewing Statistics	8-44
Viewing Service Engines and Device Group Statistics	8-44
Viewing Routing Statistics	8-46
Viewing Replication States	8-46
Viewing Proximity Engine Statistics	8-48
Viewing Overall Proximity Statistics	8-49
Viewing IS-IS Statistics	8-50
Viewing OSPF Statistics	8-51
Viewing SRP Statistics	8-53
Log Files	8-54
Transaction Logs	8-54
Transaction Log Formats for Acquisition and Distribution	8-55
Transaction Log Formats for Web Engine	8-58
Client Transaction Logs	8-58
Ingest Transaction Logs	8-65
Transaction Logging and NTLM Authentication	8-68
Usage Guidelines for Log Files	8-68
Working Logs	8-68
Archive Working Log	8-69
Exporting Log Files	8-69
Windows Media Transaction Logging	8-71

Windows Media Client Transaction Logs	<b>8-71</b>
Windows Media Ingest Transaction Log	<b>8-80</b>
Movie Streamer Transaction Log Fields	<b>8-81</b>
Flash Media Streaming Transaction Log Fields	<b>8-82</b>
Event Status Codes in Flash Media Streaming Access Logs	<b>8-86</b>
Events in Flash Media Streaming Access Logs	<b>8-88</b>
Service Router Transaction Log Fields	<b>8-89</b>
Service Monitor Transaction Logs	<b>8-90</b>
Content Manager Transaction Log Fields	<b>8-95</b>
Web Engine User Level Session Transaction Logs	<b>8-96</b>
Web Engine Custom Formats for ABR and Generic Session HTTP Transactions	<b>8-97</b>
Per Session Log	<b>8-98</b>
Snapshot Counter Transaction Logs	<b>8-100</b>

**CHAPTER 9****Maintaining the Videoscape Distribution Suite, Internet Streamer** **9-1**

Software Upgrade	<b>9-1</b>
Getting a Software File from Cisco.com	<b>9-1</b>
Pre-positioning a Software File	<b>9-2</b>
Finding the Software Version of the Devices	<b>9-3</b>
Configuring the Software Image Settings	<b>9-3</b>
Upgrading the Software	<b>9-6</b>
Downgrading the Software	<b>9-6</b>
Interoperability Considerations	<b>9-7</b>
Upgrading Software by Device Groups	<b>9-7</b>
Software Upgrades by Device	<b>9-9</b>
Rebooting Devices	<b>9-10</b>
Deleting a Device	<b>9-10</b>
Deleting a Warm Standby CDSM	<b>9-13</b>
Replacing a Device	<b>9-13</b>
Replacing a CDSM	<b>9-13</b>
Replacing an SE or SR	<b>9-14</b>
Backup and Recovery Procedures	<b>9-16</b>
Performing Backup and Restore on the CDSM Database	<b>9-16</b>
Using the Cisco VDS-IS Software Recovery CD-ROM	<b>9-17</b>
System Software Components	<b>9-17</b>
Getting the Cisco VDS-IS Software Recovery File from Cisco.com	<b>9-18</b>
Installing the Software Using the Recovery CD-ROM	<b>9-18</b>
Recovering the System Software	<b>9-19</b>
Recovering a Lost Administrator Password	<b>9-22</b>

Recovering from Missing Disk-Based Software	<b>9-23</b>
Recovering VDS-IS Network Device Registration Information	<b>9-25</b>
Disk Maintenance	<b>9-27</b>
Disk Error Handling	<b>9-27</b>
Disk Latent Sector Error Handling	<b>9-27</b>
SMART Sector Errors	<b>9-28</b>
disk repair Command	<b>9-32</b>
Removing and Replacing Disk Drives	<b>9-34</b>
Replacing a Disk	<b>9-35</b>

**APPENDIX A****Troubleshooting**

Troubleshooting Service Router Configurations	<b>A-1</b>
Troubleshooting the Distribution Hierarchy	<b>A-2</b>
Troubleshooting Content Acquisition	<b>A-3</b>
Enabling the Kernel Debugger	<b>A-6</b>
Troubleshooting Web Engine Cache Status Codes	<b>A-7</b>

**APPENDIX B****Creating Manifest Files**

Introduction	<b>B-1</b>
Manifest File Requirements	<b>B-2</b>
Working with Manifest Files	<b>B-2</b>
Specifying a Single Content Item	<b>B-2</b>
Specifying a Crawl Job	<b>B-3</b>
Understanding the Prefix Attribute	<b>B-5</b>
Writing Common Regular Expressions	<b>B-6</b>
Scheduling Content Acquisition	<b>B-6</b>
Specifying Shared Attributes	<b>B-7</b>
Specifying a Crawler Filter	<b>B-7</b>
Specifying Content Priority	<b>B-9</b>
Generating a Playserver List	<b>B-10</b>
Customized Manifest Playserver Tables and the HTTP Playserver	<b>B-11</b>
Specifying Attributes for Content Serving	<b>B-11</b>
Specifying Time Values in the Manifest File	<b>B-12</b>
Refreshing and Removing Content	<b>B-13</b>
Specifying Live Content	<b>B-14</b>
Specifying Hybrid Ingest Content	<b>B-15</b>
Manifest Validator Utility	<b>B-15</b>
Running the Manifest Validator Utility	<b>B-15</b>

Valid Manifest File Example	<b>B-16</b>
Invalid Manifest File Example	<b>B-17</b>
Understanding Manifest File Validator Output	<b>B-18</b>
Syntax Errors	<b>B-18</b>
Syntax Warnings	<b>B-18</b>
Correcting Manifest File Syntax	<b>B-19</b>
Manifest File Structure and Syntax	<b>B-19</b>
CdnManifest	<b>B-22</b>
playServerTable	<b>B-23</b>
playServer	<b>B-24</b>
options	<b>B-25</b>
server	<b>B-26</b>
host	<b>B-26</b>
proxyServer	<b>B-28</b>
item	<b>B-29</b>
crawler	<b>B-37</b>
item-group	<b>B-40</b>
matchRule	<b>B-43</b>
match	<b>B-44</b>
contains	<b>B-45</b>
XML Schema	<b>B-46</b>
PlayServerTable XML Schema	<b>B-46</b>
Default PlayServerTable Schema	<b>B-47</b>
Manifest File Time Zone Tables	<b>B-47</b>

---

**APPENDIX C****Creating Coverage Zone Files** **C-1**

Introduction	<b>C-1</b>
Zero-IP Based Configuration	<b>C-2</b>
Invalid IPv4 Addresses in Coverage Zone File	<b>C-3</b>
Coverage Zone File Example	<b>C-3</b>
Scenario 1: Coverage Zone with Client Network Only	<b>C-4</b>
Scenario 2: Coverage Zone with Geographical Location of the Datacenter Only	<b>C-4</b>
Scenario 3: Coverage Zone with Client Network and Geographical Location of the Datacenter	<b>C-5</b>
Scenario 4: Coverage Zone for Same Client Network with Different Weighted SEs	<b>C-5</b>
Scenario 5: Coverage Zone with Restricted List of SEs Used for Proximity-Based Routing	<b>C-6</b>
Scenario 6: Coverage Zone for IPv6 Client Networks	<b>C-7</b>

---

**APPENDIX D****Creating Geo/IP Files** **D-1**

Introduction	<b>D-1</b>
--------------	------------

Processing Order	<b>D-3</b>
Service Rule Config File	<b>D-3</b>
Understanding the Allow and Deny Conditions	<b>D-3</b>
Allow Conditions	<b>D-4</b>
Deny Conditions	<b>D-4</b>
Order Tag	<b>D-4</b>
Order Scenarios	<b>D-5</b>
Geo/IP File Examples	<b>D-13</b>

---

**APPENDIX E****Creating Service Rule Files** **E-1**

Introduction	<b>E-1</b>
Converting Old Service Rules to New Service Rules	<b>E-2</b>
Adding a Service Rule File to the VDS	<b>E-3</b>
Service Rule File Structure and Syntax	<b>E-4</b>
Pattern Matching	<b>E-10</b>
Rule Action Processing	<b>E-11</b>
Rule Actions for Web Engine	<b>E-12</b>
URL Resolve	<b>E-12</b>
URL Redirect	<b>E-17</b>
Force Revalidation	<b>E-17</b>
URL Generate Signature	<b>E-17</b>
URL Signing Key in the Service Rule File	<b>E-18</b>
Windows Media Streaming ASX Files with URL Signing	<b>E-20</b>
Converting Old Windows Media Streaming Service Rules for URL Signing and Validation	<b>E-25</b>
Rule Actions for Flash Media Streaming	<b>E-26</b>
Converting Old Flash Media Streaming Service Rules	<b>E-26</b>
Support for SWF Validation	<b>E-29</b>
SWF Validation Process	<b>E-29</b>
Support for DSCP Marking	<b>E-30</b>
Service Rule File Example	<b>E-31</b>
Service Rule File for URL Validation and the Exclude-Validation Attribute	<b>E-32</b>
Exclude Client IP address from URL Validation	<b>E-32</b>
Exclude Expiry Time from URL Validation	<b>E-32</b>
Exclude Both the Client IP address and the Expiry Time from URL Validation	<b>E-33</b>

---

**APPENDIX F****ABR Session-Based Encryption and Session Tracking** **F-1**

Introduction	<b>F-1</b>
HLS Session-Based Encryption	<b>F-2</b>
HLS Solution Components	<b>F-3</b>

HLS Out of Band Manifests	F-3
HSS Session-Based Encryption	F-3
Session Tracking	F-4
Session Cookie	F-4
ABR Session Tracking Client IP address Validation	F-4
Generic Session Tracking Client IP address Validation	F-4
Key Parameters	F-5
Configuring Session-Based Encryption and Session Tracking	F-5
Service Rule Configuration for Session-Based Encryption and Session Tracking	F-5
Service Rule Example for Session-Based Encryption and Session Tracking	F-6
SetParameter Names and Values	F-8
Session Resolve Rule	F-16
Session Start and Stop Notification Configuration	F-17
Key Management Server Interface	F-18
Transaction Logs for Session-Based Encryption and Session Tracking	F-21

---

**APPENDIX G****Creating NAS Files** **G-1**

Introduction	G-1
Reading NAS Metadata	G-2
Configuring NAS	G-3
NAS Mount Removal	G-3
Creating a NAS XML File	G-4
NAS XML File Example	G-4

---

**APPENDIX H****URL Signing and Validation** **H-1**

Introduction	H-1
URL Signing Components	H-1
Supported Protocols and Media	H-2
Configuring the VDS-IS for URL Signing	H-3
Configuring URL Signing	H-3
Configuring Service Rules for URL Signing	H-4
Configuring URL Signing Key	H-5
URL Signing and Validating	H-6
URL Signing Script for Symmetric Keys	H-6
URL Signing Version	H-6
Example of a Python URL Signing Script	H-7
Running a Python URL Signing Script	H-11
URL Signing and Flash Media Streaming	H-13
Importance of Device Synchronization	H-13

**APPENDIX I**

<b>CLI Commands</b>	<b>I-1</b>
Multi-Port Support	I-1
Configuring Port Channel	I-6
Redundant Dedicated Management Ports	I-6
Configuring Redundant Management Ports	I-7
Switch Port-Channel Configuration for Content Acquirer and Edge Service Engine	I-9
Verifying Port Channel Configuration	I-9
Configuring Last-Resort Routing	I-11
Configuring Standby Interfaces	I-12
Standby Interface with Switch Failover Configuration Procedure	I-15

**APPENDIX J**

<b>Verifying the Videoscape Distribution Suite, Internet Streamer</b>	<b>J-1</b>
Verifying the Web Engine	J-1
Verifying Preingested Web Content	J-1
Verifying Dynamically Ingested Web Content	J-4
Verifying the Windows Media Streaming Engine	J-9
Verifying Preingested Windows Media Content	J-9
Verifying Dynamically Ingested Windows Media Content	J-10
Verifying Windows Media Live Content Playback	J-12
Verifying the Movie Streamer Engine	J-13
Preparing Movie Streamer Content for Ingest	J-13
Verifying Preingested Movie Streamer Content	J-15
Verifying Dynamically Ingested Movie Streamer Content	J-18
Verifying Movie Streamer Live Content Playback	J-19
Verifying the Flash Media Streaming Engine	J-21
Verifying Flash Media Streaming Preingested Content	J-22
Verifying Flash Media Streaming Dynamically Ingested Content	J-26
Verifying Flash Media Streaming—Live Streaming	J-29

**APPENDIX K**

<b>Specifications and Part Numbers</b>	<b>K-1</b>
Application License	K-1
Advanced Feature License	K-2
Capacity License	K-2

Other Licenses **K-2**



## Preface

---

This preface describes the audience, objectives, organization, and conventions of the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Software Configuration Guide*. It also references related documentation and describes how to obtain documentation and submit a service request.

- [Document Revision History, page xvii](#)
- [Audience, page xvii](#)
- [Objective, page xvii](#)
- [Document Organization, page xviii](#)
- [Document Conventions, page xix](#)
- [Related Documentation, page xx](#)
- [Obtaining Documentation and Submitting a Service Request, page xx](#)

## Document Revision History

Document Version	Date	Notes
OL-32800-01	August 15, 2014	Initial release.

## Audience

This guide is for the networking professional managing the Cisco Videoscape Distribution Suite, Internet Streamer, hereafter referred to as the VDS-IS. Before using this guide, you should have experience working with Cisco IOS software and be familiar with the concepts and terminology of Ethernet, local area networking, and Internet streaming.

## Objective

This guide provides the information that you need to configure and monitor the VDS-IS.

This guide provides procedures for using the commands that have been created or changed for use with the VDS-IS. It does not provide detailed information about these commands.

This guide does not describe system messages that you might encounter or how to install your VDS-IS. See the “[Related Documentation](#)” section on page xx for links to documentation online.

For documentation updates, see the release notes for this release.

# Document Organization

Chapter or Appendix	Description
<a href="#">Chapter 1, “Product Overview”</a>	Provides a brief introduction to the VDS-IS.
<a href="#">Chapter 2, “Network Design”</a>	Describes the VDS-IS topology, elements of a Delivery Service, and the Delivery Service workflow.
<a href="#">Chapter 3, “Getting Started”</a>	Provides information about initially configuring the devices to communicate with the Content Delivery System Manager (CDSM), configuring a standby CDSM, navigating the CDSM, and a typical configuration workflow.
<a href="#">Chapter 4, “Configuring Devices”</a>	Provides information on configuring the devices in the VDS-IS.
<a href="#">Chapter 5, “Configuring Services”</a>	Provides information about configuring delivery services.
<a href="#">Chapter 6, “Configuring the System”</a>	Provides information on system configuration for the VDS-IS.
<a href="#">Chapter 7, “Configuring Licenses”</a>	Provides information on licenses for the VDS-IS.
<a href="#">Chapter 8, “Monitoring the Videoscape Distribution Suite, Internet Streamer”</a>	Provides information on monitoring the VDS-IS.
<a href="#">Chapter 9, “Maintaining the Videoscape Distribution Suite, Internet Streamer”</a>	Provides information on upgrading the VDS-IS software, deleting devices from the system, performing disk maintenance, and removing content from the system.
<a href="#">Appendix A, “Troubleshooting”</a>	Discusses troubleshooting Service Routers, and the acquisition and distribution of content.
<a href="#">Appendix B “Creating Manifest Files.”</a>	Provides information on creating and validating a Manifest file.
<a href="#">Appendix C, “Creating Coverage Zone Files.”</a>	Provides information on creating and validating a Coverage Zone file.
<a href="#">Appendix D “Creating Geo/IP Files.”</a>	Provides information on creating Authorization Service files.
<a href="#">Appendix E “Creating Service Rule Files.”</a>	Provides information on creating Service Rule XML files.
<a href="#">Appendix F “ABR Session-Based Encryption and Session Tracking.”</a>	Provides information on Session-Based Encryption and Session Tracking.
<a href="#">Appendix G “Creating NAS Files.”</a>	Provides information on creating NAS XML files.
<a href="#">Appendix H “URL Signing and Validation.”</a>	Describes the URL signing script for URL signature creation at the portal.

<b>Chapter or Appendix</b>	<b>Description</b>
Appendix I, “CLI Commands”	Provides information on configuring port channels, last resort routing domains, and other CLI commands.
Appendix J “Verifying the Videoscape Distribution Suite, Internet Streamer.”	Describes procedures for verifying the VDS-IS using different media players.
Appendix K, “Specifications and Part Numbers”	Provides information about the software licenses for the VDS-IS.

## Document Conventions

<b>Convention</b>	<b>Description</b>
<b>boldface</b> font	Commands and keywords are in <b>boldface</b> .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
Option > Option	Used to define a series of menu options.
[ ]	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 screen font.
<b>boldface screen</b> font	Information you must enter is in <b>boldface screen</b> 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.



**Note**

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



**Caution**

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



**Tip**

Means the following information might help you solve a problem.

## Related Documentation

These documents provide complete information about the VDS-IS and are available on the Cisco.com:

- *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Software Configuration Guide*
- *Cisco VDS Internet Streamer 3.0–3.1 Quick Start Guide*
- *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference Guide*
- *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 API Guide*
- *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Alarms and Error Messages Guide*
- *Release Notes for Cisco Videoscape Distributions Suite, Internet Streamer 4.0*
- *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Software Installation Guide for non-CDEs*
- *Cisco Videoscape Distribution Suite, Internet Streamer Virtualization Guide*
- *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engines*
- *Open Sources Used in VDS-IS Release 4.0*

You can access the software documents at the following URL:

[http://www.cisco.com/en/US/products/ps7127/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps7127/tsd_products_support_series_home.html)

You can access the hardware documents for the CDEs at the following URL:

[http://www.cisco.com/en/US/products/ps7126/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps7126/tsd_products_support_series_home.html)

You can access the hardware documents for non-CDEs at the following URLs:

- *Cisco UCS C200 Installation and Service Guide*  
[http://www.cisco.com/en/US/docs/unified\\_computing/ucs/c/hw/C200M1/install/c200M1.html](http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C200M1/install/c200M1.html)
- *Cisco UCS C210 Installation and Service Guide*  
[http://www.cisco.com/en/US/docs/unified\\_computing/ucs/c/hw/C210M1/install/C210M1.html](http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C210M1/install/C210M1.html)
- *Cisco UCS C220 Installation and Service Guide*  
[http://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c/hw/C220/install/C220.html](http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220/install/C220.html)
- *Cisco UCS C240 Installation and Service Guide*  
[http://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c/hw/C240/install/C240.html](http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240/install/C240.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.





## Product Overview

This chapter introduces the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS).

- [Overview, page 1-1](#)
- [Content Delivery System Architecture, page 1-5](#)

## Overview

The Cisco VDS-IS is a distributed network of Content Delivery Engines (CDEs) 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 VDS-IS supports a variety of mechanisms to accelerate the distribution of content within the content delivery network. It also offers an end-to-end solution for service providers to ingest and stream entertainment-grade content to subscribers.

The VDS-IS functionality can be separated into four areas:

- Ingest
- Distribution
- Delivery
- Management

Each CDE in the VDS-IS 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 Internet Streaming Content Delivery System Manager (CDSM) device names.

**Table 1-1      CDA Mapping to Functionality and CDSM**

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

The Service Engine can function as a Content Acquirer and Internet Streamer, or just as an Internet Streamer.

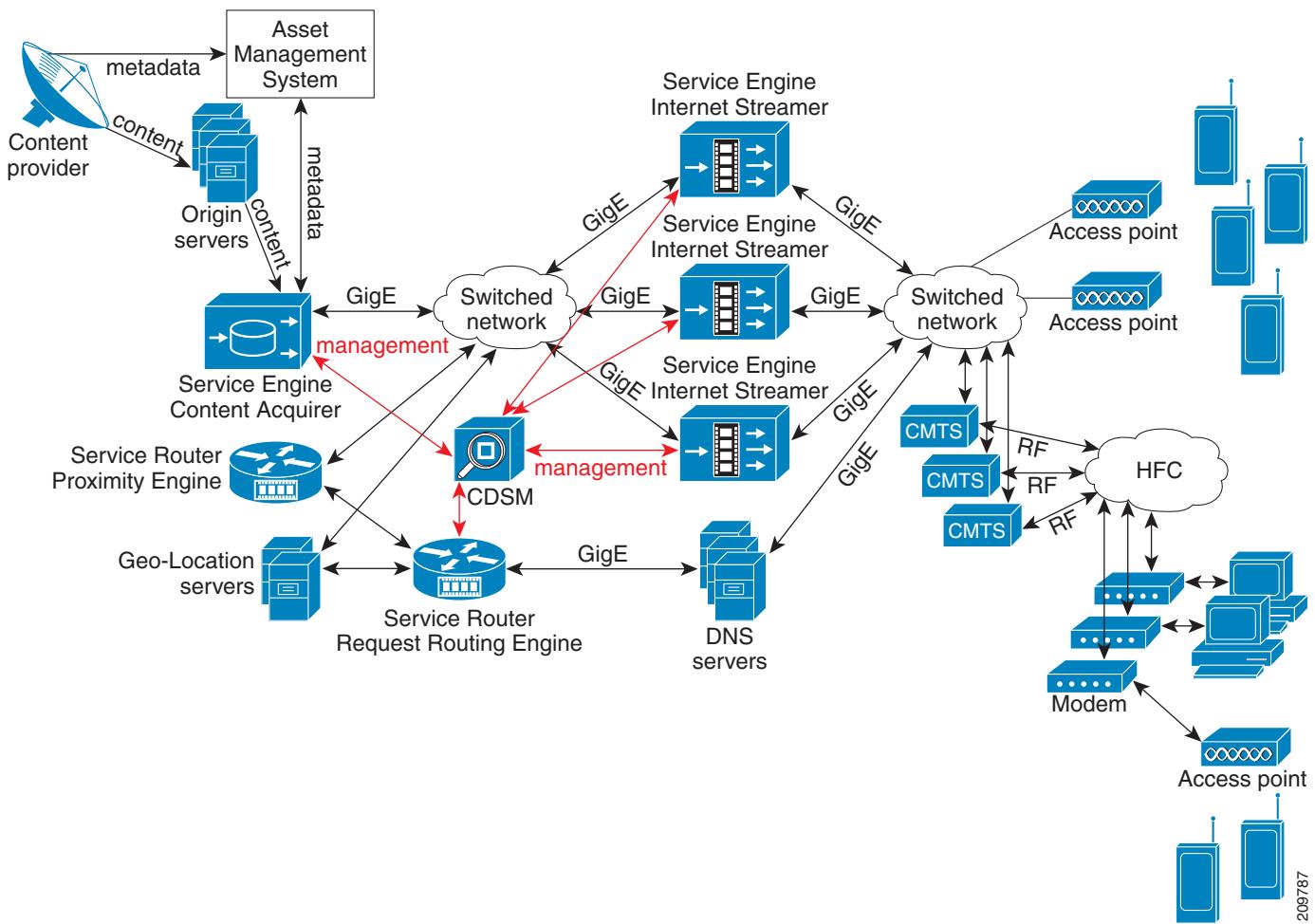
**Overview**

Figure 1-1 shows the major elements of a VDS-IS network. How content flows, from ingest to distribution within the VDS-IS, 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 are as follows:

- 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 VDS-IS



The following sections briefly describe the elements of the VDS-IS. For more detailed information, see the “Content Delivery System Architecture” section on page 1-5.

## Ingest and Distribution

The Service Engine designated as the Content Acquirer for a Delivery Service is the ingest device. VDS-IS supports the following methods of content ingest:

- Prefetch ingest
- Dynamic ingest
- Hybrid ingest
- Live stream ingest and split

The distribution of content within the VDS-IS is determined by the method of ingest used.

### Prefetch Ingest

The Content Acquirer receives metadata from the back-office in the form of an XML-formatted Manifest file, and using the information in the file, pulls the content into storage on the Content Acquirer. The content can be ingested by using different protocols. The supported protocols are FTP, HTTP, HTTPS, and CIFS, 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 content type (MIME) value cannot exceed 32 characters.

---

### Dynamic Ingest

Content can be dynamically ingested into the VDS-IS. Dynamic ingest is triggered when a Service Engine's Internet 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 VDS-IS network. Content ingested and distributed by this method is deleted if clients do not request it frequently.

The Internet Streaming CDSM manages this ingest method internally, not by instructions embedded in a Manifest file, and manages the storage automatically. The Internet Streaming 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.

## Live Stream Ingest and Split

The live stream ingest method distributes a live content feed to all of 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 Internet Streamer application and optimizes the access by doing a one-to-many split to all Service Engines in the content Delivery Service. The Internet Streaming CDSM 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.

[Table 1-2](#) lists the content types and formats, content transport protocols, and client types supported by the VDS-IS.

**Table 1-2      Supported Content Types**

Content Types and Formats	Transport Protocols	Typical Client Types	Access Network Type
Windows Media (WMA, WMV, ASF, and others) VC-1	RTP, RTSP, HTTP	Windows Media Player 9, 10, 11 on PC Windows Media Player 9 for Mac Windows Media Technology (WMT) Silverlight	Wired Wi-Fi Cellular
QuickTime (MOV), hinted (3GP) files	RTP, RTSP, HTTP	On PC: QuickTime Player, QuickTime Pro 6 or 7, RealPlayer 10 or 11 (3GP only), VLC player On Mac: QuickTime Player, QuickTime Pro 6 or 7, RealPlayer 10 for Mac OS X (3GP only)	Wired Wi-Fi Cellular

**Table 1-2 Supported Content Types (continued)**

<b>Content Types and Formats</b>	<b>Transport Protocols</b>	<b>Typical Client Types</b>	<b>Access Network Type</b>
Other Hypertext and image files (HTML, JPEG, and so on)	HTTP	Web browsers and other HTTP clients	Wired Wi-Fi Cellular
MPEG (MP1, MP2, MP4)	RTP, RTSP	MPEG clients  <b>Note</b> For Flash Media Streaming, the Adobe Flash Media Player 9 update 3, Adobe Media Player, and Adobe Air, are the only players that support MPEG-4.	Wired
Adobe Flash (SWF, FLV, MP3)	RTMP, HTTP	Adobe Flash Player 9 for Windows, Mac OS, and Linux	Wired Wi-Fi Cellular
H.264	RTMP, HTTP	H.264 clients  <b>Note</b> For Flash Media Streaming, the Adobe Flash Media Player 9 update 3 is the only supported player.	Wired

**Note**

RTMP is part of the Flash Media Streaming feature.

## Management

The Internet Streaming CDSM, a secure web browser-based user interface, is a centralized system management device that allows an administrator to manage and monitor the entire VDS-IS network. All devices, Service Engines and Service Routers, in the VDS-IS are registered to the Internet Streaming 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 Internet Streaming CDSM also provides an automated workflow to apply a software image upgrade to a device group.

## Content Delivery System Architecture

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

- [Service Engine](#)
- [Service Router](#)

## Content Delivery System Architecture

- Content Delivery System Manager
- Resiliency and Redundancy

## Service Engine

Each Service Engine can function as a Content Acquirer and Internet Streamer, or just as an Internet 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 Internet Streamer.

## Storage and Distribution

Both the Content Acquirer and the Internet Streamer applications have storage and distribution functions within the VDS-IS, which include the following:

- Management of the physical storage of content and metadata. 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 accessed frequently. 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 VDS-IS topology and all of 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.

## FastCAL

The Content Abstraction Layer (CAL) library provides an interface to the Content Delivery Network File System (CDNFS). The CAL library monitors the content in the CDNFS and communicates with the Content Manager process to evict less popular content.

The Fast Content Abstraction Layer (FastCAL) library provides quick response time for high-performance Web Engine create, update, lookup, and delete operations. All other protocol engines and modules, including live streaming for Flash Media Streaming and RTSP gateway, continue to use the CAL library and Unified Namespace (UNS) process. Flash Media Streaming VOD (prefetched, hybrid and dynamically cached content) use FCAL by way of the Web Engine. FastCAL communicates with the Content Manager for popularity tracking. Lookup notifications are also sent from FastCAL to the Content Manager.

### Disk Path

FastCAL creates the disk path for cache content. An example of a disk path with an HTTP content URL of <http://192.168.1.9/vod/foo.flv> follows:

/disk11-01/c/192.168.1.9/1d/a1/1da1394af838bbcb45af78fd5681abeb/foo.flv.http

The disk path for the prefetched HTTP content URL, http://192.168.1.9/vod/c5.flv, translates to the following:

/disk03-01/p/192.168.1.9/1d/a1/1da1394af838bbcb45af78fd5681abeb/c5.flv

### Disk Allocation

Disk usage for all disks is maintained in shared memory, which is updated by the Content Manager with actual disk usage and by FastCAL when new content is created. FastCAL creates predefined *buckets*, which are groups of disks. The number of disks per bucket varies, and the number of buckets varies; it is determined by the CDE model.

The CDNFS disk mount point is always displayed as disk-YY, where **XX** is the disk number and **YY** is the partition. Every content URL is always associated with the same bucket, so lookup, create, and delete always happen within the same bucket. This method avoids searching all disks on the CDE. If a bucket has no disks (because of disk failure, unmounting of the disks, and so on), content is served from the network. The incoming traffic to the SE is distributed evenly to the buckets, which means that if the number of available disks in a bucket is less than the other buckets, the other disks in the impaired bucket are used more, which may impact performance.

### Bucket Allocation

A hashing algorithm is used to generate a hash of the content URL, on which a calculation is performed to determine the bucket for the content. This ensures content is distributed evenly among all of the buckets.

## Content Manager

The Content Manager module keeps track of all the files in CDNFS, and maintains all content popularity information and stores it in a snapshot file. the Content Manager includes the following enhancements:

- Improved the cache content storage:
  - For a platform with physical memory size less than 32GB(33,554,432KB), the maximum cached file entries is 20 million and the maximum cached directories 1 million.
  - For a platform with physical memory size more than 32GB(33,554,432KB), the maximum cached file entries is 50 million and the maximum cached directories 10 million.
- Increase maximum length of URL to 2048 characters



**Note** In calculating the maximum length of the URL (2048 characters), an MD5 hash must be considered as part of the overall URL length, therefore the maximum length of the URL should not exceed 2028 characters.

- Continue to manage cache content objects for all protocol engines
- Maintains share memory containing disk related information
- Monitors disk usage periodically and starts eviction when usage exceeds threshold
- Receives updates on disk information based on CMGRSlowScan process, which scans the entire system after every Primary start-time of slowscan. The Primary start-time of slowscan (or Secondary start-time of slowscan) is set in the Devices > Devices > General Settings > Content Management page in the CDSM GUI.
- Receives updates on each disk during start-up from CMgrSnapshotReader.

**Note**

We recommend that any CDE model that has hard-disk drives (HDDs) instead of solid-state drives (SSDs), and is used to stream ABR content, be configured with a maximum of 5 million objects instead of the 20 million objects. This is because HDD-based hardware requires more seek time to access content. The software can handle 20 million objects, but the hard-drive access time impacts the ABR streaming performance. ABR content consists of a large number of small files, which results in a lot of overhead.

For long-tail content (Windows Media Streaming, Flash Media Streaming, Movie Streamer, and progressive download), the maximum number of content objects can be configured with the default of 20 million objects on HDD-based hardware models.

Two of the HDD-based hardware models are the CDE220-2G2 and CDE250-2M0.

**Content Types**

The Content Manager manages content object types in the following ways:

- Cache content—Maintains file information such as disk path, file size, and priority
- Prefetched content—Maintains prefetched file disk path in memory to manage the number of prefetched assets in the system
- Hybrid content—Handles the same as cache content, maintains file information
- Related content—Maintains information on parent content disk location, aggregated size and hit count

**Create**

When a file is created (added), FastCAL library updates the Content Manager with the file location, URL, file size, and hit counts.

If the cache-fill rate (creation rate) is much faster than the deletion rate, the Content Manager sets the unwritable flag for that disk. If a protocol engine wants to create content in the system, FastCAL avoids using that disk for the file creation. If all disks are unavailable, the protocol engine performs a bypass or cut-through operation.

The Content Manager sets the disk unwritable flag for the following reasons:

- Disk usage reaches the DiskStopCreate high watermark (98 percent)
- Total cache content objects reaches the ObjCntStopCreate high water mark (105 percent)
- Deletions exceeds 5000 entries

The Content Manager removes the disk unwritable flag when the following occurs:

- Disk usage is below the DiskStartCreate low watermark (95 percent)
- Content object count is below the ObjCntStartCreate low watermark (100 percent)
- Deletion entries drop below 5000

The status of whether the cache content can be stored is displayed in the **show cdnfs** command.

**Update**

The Content Manager monitors the cached and prefetched content, but not live content. FastCAL updates the content creation time (if created), hit count, file size, and disk path information in the Content Manager when there is a popularity update call from the protocol engine. Whenever there is a cache content popularity update, the Content Manager stores the popularity information and the file path of the

content, and computes the popularity (priority) of the content. If the update is a prefetched content popularity update, the Content Manager ignores the message, but continues to monitor the prefetched URL for statistics.

Because of the Web Engine's capability to request bundling, multiple requests can be served by a single datasource. The datasource keeps track of the requests that are served from it and calls the popularity update at the end of its lifecycle (before eviction of the datasource).

### Delete and Eviction

Deletion operating is when a file is deleted through the CLI or by the protocol engine. The FastCAL library deletes the content object from the disk first, then sends a message to the Content Manager to remove the entry for the deleted content object. If the message is lost, the Content Manager deletes the entry by way of the sanity check which runs after Slow Scan (CMGRSlowScan) is finished or through the eviction process.

The Content Manager is involved in evicting content. If the disk usage high-watermark is reached, the Content Manager starts the eviction process by deleting cached content with the lowest priority first. If the protocol engine uses FastCAL to delete the content, FastCAL deletes the content and updates the Content Manager.



#### Note

The disk path is maintained in a hierarchical manner by breaking down disk path with the directory node (Dir Node) and file node (File Node). If the number of Dir Nodes exceeds the limit (one million), the Content Manager starts evicting files in a similar process to object count eviction.

### Priority Calculation

The priority calculation is based on the current hit count, the size of the content object, and the decay of the content object. The popularity of the content decays over a period of time if the content is not accessed.

By default, the Content Manager prefers to keep small content objects over large content objects, because the overhead of fetching a small object is higher than larger objects. However, this preference is configurable in the following ways:

- CDSM GUI: By choosing the Devices > Devices > General Settings > Content Management page, Cache content eviction preferred size drop-down list.
- CLI: By using the cache content eviction-preferred-size {large | small} command.

## Deletion Scenarios

There are five scenarios in which the Content Manager removes content:

1. The disk usage exceeds threshold.
2. Content objects exceed the **cache content max\_cached\_entries** command value.
3. The Cached directories exceed the **cache content max-cached-dirs** command value.
4. The Delivery Service or SE is removed from the CDSM GUI.
5. The disk is removed or marked as “bad.”
6. The **clear cache all** command is entered.

The first two can be categorized as priority-based content eviction, the following two can be categorized as top-down tree-structure deletions, and the last one can be categorized as a forking deletion. In all scenarios, the Content Manager removes all entries for the associated content, and deletes all content from storage (with the exception of disk removal).

### Disk Usage Exceeds Threshold

The Content Manager keeps track of disk usage. If the disk usage reaches the disk usage high watermark (93 percent), the Content Manager starts the eviction process. When the disk usage reaches the disk usage low watermark (90 percent), the eviction process stops. The eviction process is based on the following criteria:

- Priority of the content on each disk
- Available space on each disk

### Content Count Exceeds Maximum Allowed

The default maximum numbers of cached entries and directories depend on the platform. If the maximum is exceeded for max-cached-entries or max-cached-dirs, the Content Manager starts the eviction process.

### Delivery Service or SE Removal

If a Delivery Service is removed from the CDSM or an SE is deregistered from a Delivery Service, the Content Manager creates a deletion task and starts deleting all associated cache content. For prefetched content, the Content Manager removes all references, and Acquisition and Distribution handles the content object deletion.

### Disk Removal or Disk Marked as Bad

If a disk has gone “bad” and is removed from the system, UNS is notified. UNS internally calls FastCAL, which notifies the Content Manager. The content object information is removed from the Content Manager. The Content Manager also monitors the disk status every three seconds, and if a disk is removed, the Content Manager removes all associated entries for it.

#### **clear cache all Command**

If the **clear cache all** command is entered, the Content Manager creates a child process to delete the cache content. The progress of the clear cache all operation is shown in the **show cache** command output.

### Addition and Deletion Processes

Content addition stops at 105 percent of the maximum object count or 95 percent of the CDNFS capacity (disk usage). For example, if the maximum number of objects has been configured as 20 million, the VDS-IS starts deleting content if the object count reaches 20 million, but adding content is still allowed. Adding content stops when the maximum number of content objects reaches 21 million(105 percent of 20 million), which allows time for the content deletion process to reduce the number of objects in the VDS-IS to the configured limit. Adding content resumes only after the number of objects is 20 million or less. The same logic applies to disk usage. The deletion process starts when the disk usage reaches 93 percent, adding content stops when the disk usage reaches 98 percent, and adding content resumes only after the disk usage percentage reaches 95 percent or less.

If adding content has been stopped because either the content count reached 105 percent of the limit or the disk usage reached 98 percent of capacity, the unwritable flag is set in the share memory and when the protocol engine calls create, FastCAL library looks into the share memory and denies the creation request. The protocol engine performs a bypass or cut-through operation.

The **show cdnfs usage** command shows the current status of whether the content is able to be cached or not.

The following is sample output from the **show cdnfs usage** command:

```
# show cdnfs usage
Total number of CDNFS entries : 2522634
Total space : 4656.3 GB
```

```
Total bytes available      : 4626.0 GB
Total cache size          : 2.4 GB
Total cached entries      : 2522634
Cache-content mgr status  : Cachable
Units: 1KB = 1024B; 1MB = 1024KB; 1GB = 1024MB
```

If the maximum object count is reached, the following is displayed:

```
Cache-content mgr status: Not cacheable on the following disk(s): [/disk00-06]
[/disk01-06] [/disk02-01]
105% of max obj count reached :      [/disk00-06] [/disk01-06] [/disk02-01]
```

If the disk usage reaches more than 98 percent, the following is displayed:

```
Cache-content mgr status: Not cacheable on the following disk(s): [/disk01-06]
[/disk02-01]
98% of disk usage reached:      [/disk01-06] [/disk02-01]
```

Starting with Release 3.3, VDS-IS supports content deletion per Delivery Service and per Service Engine by using wildcards. To remove the cached content in SEs, you need to use the CLI, CDSM GUI, or the API to request a content deletion task.

For each URL, the deletion request will be sent to all Service Engines assigned to the Delivery Service by default. It is also possible for the user to select specific Service Engines to delete content on.

If a Delivery Service or content origin is deleted, all of its cached content will be automatically deleted; the user will not need to manually delete contents for a non-existing Delivery Service or content origin.

For more information on content deletion and deletion tasks, see the “[Processing Content Deletion](#)” section on page 8-34.

### Eviction Protection

The Content Manager provides configurable eviction protection for small size content and large size content. The Content Manager eviction algorithm is triggered when the disk usage reaches 93 percent or when the cached object count reaches the configured maximum object count. The eviction algorithm assigns a priority number to each content object based on an algorithm similar to the greedy-dual-size-frequency (GDSF) algorithm. The priority number is based on the size and usage of the object. Small objects are given preference over large objects; that is, they are less likely to be deleted.

To protect incoming small objects from being deleted, use the **cache content small-file-eviction-protection** global configures command. The **cache content small-file-eviction-protection** command allows you to set the maximum content size (500 KB, 1 MB, 2 MB, 4 MB, 10 MB and 20 MB) and the minimum age (5, 10, 15, 30 minutes) of the content object to be protected from deletion. For example, to set the eviction protection for content objects smaller than 20 MB that were ingested in the last 30 minutes, you would enter the following command:

```
#(config) cache content small-file-eviction-protection max-size-20MB min-duration-30min
```

If the content object being cached is smaller than the configured size, it is inserted into a protection table along with the current time stamp. If the difference between the object's time stamp and the current time is greater than the configured time duration, the object is removed from the protection table.

To protect incoming large objects from getting a low priority and being deleted, use the **cache content eviction-protection** global configure command. The **cache content eviction-protection** command allows you to set the minimum content size (100 MB, 500 MB, 1 GB, and 4 GB) and the minimum age (1-4 hours for 100 MB size, 1, 4, 8, or 24 hours for all other sizes) of the content object to be protected from deletion. For example, to set the eviction protection for content objects larger than 100 MB that were ingested in the last two hours, you would enter the following command:

```
#(config) cache content eviction-protection min-size-100MB min-duration-2hrs
```

## Content Delivery System Architecture

If the content object being cached is larger than the configured size, it is inserted into a protection table along with the current time stamp. If the difference between the object's time stamp and the current time is greater than the configured time duration, the object is removed from the protection table.

When the eviction algorithm is triggered, before it selects an object for deletion, it first looks at the protection table, and if the object is found, it is skipped for that iteration. The **clear-cache-content** command also checks the protection table before deleting an object. The **clear-cache-all** command does not check the eviction protection table; only the cache content is deleted. As for relative cache content, content in the protection table might still be deleted if the relative content is not protected. The small content eviction protection and large content eviction protection is disabled by default.

If the Content Manager eviction algorithm is not able to find any content to delete, a syslog message is sent to notify the administrator to revisit the configuration. Changing the settings of the **cache content small-file-eviction-protection** or **cache content eviction-protection** command only affects the content that is currently in the protection table and any new content that is added. Any object that is removed from the protection table prior to the configuration change is not brought back into the protection table.

The **no cache content small-file-eviction-protection max-size-xx duration-xx** command removes all small content protection entries in the eviction protection table. The **no cache content eviction-protection min-size-xx duration-xx** command removes all large content protection entries in the eviction protection table. Reloading the SE clear all entries in the eviction protection table.

## Web Engine Integration with FastCAL

The Web Engine calls FastCAL directly for content creation, lookup, update, and deletion.

### CAL Queue Limits

The CAL queue is limited to 3000 tasks on the CDE250 and 1500 tasks on all other CDEs. When the CAL queue threshold is exceeded, the Web Engine does not add anymore disk operation tasks (creates, updates, or popularity updates) and a trace message is logged with the following string:

Reason: CalQThreshold Exceeded!

A new output field, “Outstanding Content Popularity Update Requests,” has been added to the **show statistics web-engine detail** command. At any point, the sum of the “Outstanding Content Create Requests,” “Outstanding Content Update Requests,” and “Outstanding Content Popularity Update Requests,” output fields is always less than the threshold. If the sum of these three output fields exceeds the CAL queue threshold, no more create, update, and popularity update tasks are performed, the “Reason: CalQThreshold Exceeded!” trace message is logged, and content is served as follows:

- Large content files are served by way of bypass
- Small content files are served from tmpfs and the files are evicted from tmpfs without moving them to disk

## UNS Integration with FastCAL

UNS is the process that is called by other modules like CMS, Acquisition and Distribution, and Streamscheduler to access the CDNFS content by way of the CAL-UNS client library. UNS still handles Movie Streamer and Windows Media Streaming content (both prefetched and cached), and live streaming content for Flash Media Streaming.

UNS uses FastCAL for any disk-based operation. The Content Manager and FastCAL handle accounting of disk usage and new content allocation to the disks for all modules.

## Stream and Cache-Fill Performance

The Stream and Cache-Fill feature improves performance in the following ways:

- QoS support. Using QoS together ensures that sessions receive either best effort or a guaranteed rate while not exceeding overall system capacity.
- File-level hole management is supported, allowing partially-filled files to be streamed, and multiple-parallel fills and streams to be attached to the same file at various offsets.
- Higher performance data transmission engine provides better throughput

Hole management is not used for small files, because the sessions are over quickly, and the entire file is always downloaded from the Origin server. Encrypted HLS traffic and HTTPS traffic do not use the Stream and Cache-Fill components, because HTTPS traffic is encrypted in the user space, and encrypted HLS traffic is similar to small ABR files.

With ABR large files, files are either stitched from fragments or they are natively large files. Clients are more likely to stop streaming from an ABR large file when they shift bit rates, so files may have holes.

Hole management and QoS optimize the serving of large ABR files. There is a large improvement in performance with ABR large files and the Stream and Cache-Fill feature.

Large file progressive download traffic is similar to large ABR files, but the client is likely to stay on a bit rate longer because it does not automatically adjust its rate. This traffic type also sees a large performance improvement, for the same reasons as large ABR files.

## Stream and Cache-Fill Feature Components

The Stream and Cache-Fill feature consists of the following components:

- [QoS Types, page 1-13](#)
- [Hole Management, page 1-14](#)

### QoS Types

The Stream and Cache-Fill feature adds support for the following QoS classes:

- Hard Guaranteed (HG)—Flows assigned a bit rate that is maintained under any circumstances. The bandwidth allocated for these sessions is never reused by other sessions. HG is not directly selectable.



**Note** HG is not supported in Release 3.1.

- Soft Guaranteed (SG)—Flows assigned a fixed bit-rate, unlike HG, any unused bandwidth assigned can be reused by other sessions. SG and best effort (BE) flows can continue to be admitted even if the total requested SG rate exceeds system capacity, as long as the total measured rate does not exceed the total system capacity. This is a *statistical guarantee* in the sense that it is expected to be guaranteed in most circumstances.
- Best Effort (BE)—Depending on whether the traffic is VOD or live, the bandwidth allocation behaves differently.
  - In the VOD case, all BE streams are given an equal share of any disk bandwidth left over after guaranteed sessions are satisfied.
  - In the live case, each BE client is allowed to stream at a rate limited only by CPU and network interface bandwidth.

The system has an administratively-defined minimum best-effort rate for VOD BE sessions. New sessions are only admitted if the global best-effort rate does not fall below the minimum. This way the SE does not stream countless sessions at very low bit-rates.

- On any given SE, live BE traffic cannot be mixed with any other type of QoS, but VOD BE can be mixed with guaranteed QoS types.

**Table 1-3** summarizes the different QoS types in the VDS-IS. The types listed in bold are introduced with this feature.

**Table 1-3      Supported QoS Types**

<b>QoS Type</b>	<b>Minimum Guaranteed Rate</b>	<b>Maximum Rate</b>	<b>Other Compatible QoS Types</b>
<b>Hard Guaranteed (HG)</b>  (not supported in Release 3.1)	Protocol Engine requested rate	Protocol Engine requested rate	SG, BE
<b>Soft Guaranteed (SG)</b>	Delivery service bitrate	Delivery service bitrate	HG, BE
<b>Best Effort VOD (BE-VOD)</b>	Globally configured minimum	(Total disk rate - Total (SG + HG) rate) / number BE sessions	SG
Best Effort Live (BE-live)	None	Determined by CPU and network cards	None
Fixed Bit Rate	None	Delivery service bitrate	None
Best Effort	None	Determined by CPU, network cards and disk	None

There is no performance penalty for using any QoS type. The QoS types are defined indirectly through the delivery services.

QoS statistics can be viewed by using the **show statistics admission** command.



#### Note

Only admission statistics can be cleared. QoS statistics are dynamically measured quantities rather than counters; and therefore, cannot be cleared.

### Hole Management

Although hole management is not directly visible as a feature to the user, it has a great impact on system behavior. The basic ideas of hole management are as follows:

- Multiple fills can run on a single file at different offsets
- Play request is considered a hit either if the entire request range is filled, or a currently active fill will eventually fill that range
- Maximum number of holes per file is limited for file system robustness reasons

Holes in a file are created in two cases:

1. If the last client aborts the session and fills are still going to the file.
2. When fills are aborted for some other reason like the Origin server drops the connection.

In either case, hole management is equipped to handle these holes by starting fills as needed to bridge holes and limit the total number of holes in a file if required.

When a client aborts a session, any associated fill task normally continues to completion, until either the entire hole is filled or until the end of file. The exception to this is when no more clients are playing the file. In this case, all fills are aborted.

## NAS

Network-attached Storage (NAS) is supported as a read-only storage repository at the root location (Content Acquirer) in the VDS-IS. Content is written to NAS by an external agent, such as the Origin Server, a publishing subsystem, or a data storage application. NAS offers a new content category, similar in characteristics to dynamically-cached content, which does not require metadata attachment.



**Note** NAS is only supported in lab integrations as proof of concept.

The following rules apply to NAS support:

- NAS cannot be used as a source for prefetched or hybrid content.
- Only content serviced by the Web Engine is supported (HTTP content and Flash Media Streaming).



**Note** NAS for Windows Media Streaming and Movie Streamer is not supported.

- Only Network File System (NFS) mounts are supported for acquiring content from NAS.
- Content acquired from NAS is not written to local storage on the SEs at the root location; when reading content, NAS is considered an extension of the local file system.
- If there is more than one SE at a root location for a Delivery Service, then the SE that acquires the content from NAS is based on a hash of the content URL (similar to dynamically-cached content).
- NFS share can be mounted from multiple IP addresses simultaneously.
- Multiple mounts for the same volume on a NAS is supported.
- NAS should be collocated with the SEs at the root location; if WAN link is used, then WAN link failover scenario should be provided.
- IP address failover by NAS should be implemented to avoid service disruption.
- NAS is not applicable to live streaming.
- NAS lookup is tried before pulling content from the Origin Server.
- When the Web Engine performs FastCAL lookup, NAS file lookup is performed first; followed by cached content, then prefetched content.
- In a cache-miss scenario, the Origin Server is queried last.



**Note** Ingress traffic from NAS mounts is not distributed evenly over port channels. Separate interfaces can be used for NAS outside of the port-channel configuration to achieve better load balancing. Ingress traffic to the VDS-IS is determined by the switch, this applies to all application traffic over port channels.

## 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, FTP, or CIFS (Dynamic ingest supports HTTP only).
- 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.

Starting with Release 3.2.2, when the Content Acquirer sends a request to the Origin Server and when the Content Acquirer distributes the content through multicast, Differentiated Services Code Point (DSCP) marking is done on the outgoing content request to the Origin Server and on the data distributed through multicast to other Internet Streamers.

**QoS value for content ingest and QoS value for multicast data** set in **Delivery Services Definition** page in CDSM GUI are used as DSCP values when the Content Acquirer does content ingest from the Origin Server and when the Content Acquirer does content distribution to other Internet Streamers respectively.



**Note** Starting with Release 3.3.0, VDS-IS supports per-session DSCP marking for Flash Media Streaming for both VOD and live which is configured differently by Service Rule file.

## Internet Streamer

All Internet Streamers participating in a Delivery Service pull the metadata from a peer Internet Streamer called a *forwarder*, which is selected by the internal routing module. Each Internet Streamer participating in a Delivery Service has a forwarder Internet Streamer. The Content Acquirer is the top-most forwarder in the distribution hierarchy. In the case of prefetched ingest, each Internet 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 an Internet Streamer, the protocol engine application gets the information about the set of upstream Internet Streamers through which the content can be acquired. In the case of dynamic ingest, the Internet 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 Internet 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. Windows Media Engine, Movie Streamer Engine, and Flash Media Streaming engine support live stream splitting.



**Note** VDS-IS Release 3.2.2 supports only prepositioned content and does not support Live Stream, Windows Media Engine, Movie Streamer Engine, and Flash Media Streaming because this release is primarily intended for VOD applications.

The Internet Streamers use service control to filter and control incoming requests for content. The Service Rules and Authorization Server with IP address and geographic-location blocking are some of the functions that are encapsulated under the Service Control option in the Internet Streaming CDSM.

The Internet Streamers send keepalive 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 Internet Streamer to handle the request.

Starting with Release 3.2.2, when the receiver sends a NAK packet to the sender for any missed data packets, Differentiated Services Code Point (DSCP) marking is done on the NAK packet sent.

The DSCP value is obtained from the value set for **QoS value for multicast data** set from the **Delivery Services Definition** page in the CDSM GUI is used as DSCP value when the receiver sends NAK packet to the sender.

The Internet Streamer function is implemented as a set of protocol engine applications. The protocol engine applications are as follows:

- [Web Engine, page 1-17](#)
- [Windows Media Streaming Engine, page 1-21](#)
- [Movie Streamer Engine, page 1-26](#)
- [Flash Media Streaming Engine, page 1-28](#)

## Web Engine

All HTTP 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, can serve the request from locally stored content in the VDS-IS or from any upstream proxy or origin server.

An HTTP 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 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. The message size between Web Engine and Windows Media Streaming is 12 KB.

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.

Starting with Release 3.2.2, when the Web Engine requests content from the Origin Server, DSCP marking is done on the outgoing content request from Web Engine to Origin Server. The Web Engine uses the **QoS value for content ingest** value set in **Delivery Services Definition** page in CDSM GUI when it does content ingest from the Origin Server.



### Note

The Web Engine supports the following:

- Optimization for small content objects
- Optimization of Adaptive Bitrate Streaming for Movie, Apple iPhones, and Smooth HD
- Movie video on demand (VOD) streaming
- Movie live streaming
- MP3 live streaming

- Interoperation with Apple's media stream segmenter, as well as Microsoft's Internet Information Services 7.0 (IIS7.0) Smooth Streaming.
  - Apple's media stream segmenter segments encoded media into separate files for streaming to iPhones.
  - Microsoft's IIS Smooth Streaming offers adaptive streaming of high-definition (HD) content.
- HTTP GET and HEAD request methods.

Bursts of traffic (such as 800 connections per second) may cause the Web Engine to become disabled before it can transmit notification to the SR that the threshold has been reached.

When the content file is smaller than the chunk size, the Unified Kernel Streaming Engine (UKSE) sends the entire file immediately. In this case, the UKSE does not check pacing; therefore, the bit rate for files smaller than the chunk size is not honored.

---

### Cache-Fill Operations

The Web Engine communicates to the upstream Service Engine for cache-fill operations. This interaction is based on HTTP. This cache-fill operation is on demand and therefore 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 Internet Streaming 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.



**Note**

When cache-control:no-store is sent in a 200 response from the Origin server, the Web Engine respects the no-store header and does not cache the content. However, if no-store is appended to the cache-control header in a 304 response, the no-store header does not trigger deletion of the content from the disk. The 304 response only triggers updating the cache with the recent header attributes sent in the 304 response header.

The Web Engine supports request headers and entity headers as described in the HTTP 1.1 specification (RFC 2616). The Web Engine allows VDS-IS domain and HCACHE custom headers only when sent from an SE.

Web Engine respects the following date formats:

- Sun, 06 Nov 1994 08:49:37 GMT ; RFC 822, updated by RFC 1123
- Sun Nov 6 08:49:37 1994 ; ANSI C's asctime() format

The following format is obsolete and is not supported:

- Sunday, 06-Nov-94 08:49:37 GMT ; RFC 850, obsoleted by RFC 1036

If the headers (for example, the expiry header) are received with a non-supported date format, the Web Engine continues to cache the content, but subsequent requests for the same URL are revalidated as the content is considered expired.

---

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. If the Web Engine performs the calculation and determines that the content should be checked for freshness with the origin server, and the origin server is unreachable, the client receives a 504 error.

**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 used 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.

Revalidation is enabled by default for the Web Engine.

---

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 VDS-IS 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 that 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* 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:

$\text{Cache\_age} = \text{Current\_time} - \text{Create\_time}$

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:

$\text{Response\_delay} = \text{Create\_time} - \text{Time\_request\_sent\_to\_origin\_server}$

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 VDS-IS 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.

### **Dynamic Caching**

Starting with Release 3.2.2, dynamic caching is configurable per Delivery Service. By default, dynamic caching is enabled. If a content requested by the client is not present in the cache then the Web Engine sends a request to an upstream streamer to acquire the contents, caches the contents and then delivers it to the client.

By making the dynamic caching configurable at Delivery Service level, the user has the option of disabling the lookup from the origin server.

If the requested content is not available in a particular streamer or service engine, and dynamic caching is disabled, the client receives a 403 error response (HTTP FORBIDDEN).

The dynamic caching feature is configured in the Services > Service Definition > Delivery Services > General Settings page in the CDSM GUI.

If dynamic caching is disabled, only prepositioned content and contents cached before dynamic caching was disabled for which cache revalidation is not required will be served to the client.

The dynamic cache setting for a given Delivery Service will override the following configuration properties:

- The web-engine cache settings for age-multiplier, max-ttl, min-ttl will not be affected by dynamic caching configuration.
- The web-engine revalidation setting will be overridden by the dynamic cache setting for a given Delivery Service. No cache revalidation will be done if dynamic caching is disabled for the contents pertaining to that Delivery Service. If the complete content is available, it is served without any revalidation.
- The cache bypass requests will not be processed if dynamic caching is disabled.
- If dynamic caching is disabled and only partial content is available, then client receives a 403 error message.

### **Per-Request HTTP Headers from Redirected URLs**

When the VDS-IS is integrated with products such as the Content Adaptation Engine (CAE), Service Engines are used to serve over-the-top content. In such scenarios, the VDS-IS provides HTTP headers similar to that of the Origin server. The information in the HTTP header can be unique to a user session.

The CAE retrieves this information from the Origin server response and provides it as a query parameter within the URL. This information is intact when received by the Service Engine following redirections from the CAE and Service Router. The Web Engine retrieves the “\_resp\_hdrs\_” value from the received URL. The retrieved value is % unescaped, and parsed for use when serving the content.

As indicated in RFC 2396, a query parameter cannot contain the reserved characters ;?:@&=+,,\$ and thus are escaped using % encoding. The query string must have the “\_resp\_hdrs\_” tag. A URL with the “\_resp\_hdrs\_” tag has the following format:

http://<URL to serve>?\_resp\_hdrs\_=<strings to include in the http headers>

The following is an example of a URL with the “\_resp\_hdrs\_” tag and value:

http://nas\_url\_to\_serve?\_resp\_hdrs\_=Set-Cookie%3A%20ff%3DrlsBo4v%3B%20path%3D/%3B%20domain%3D.site.com

### HTTP Error Response Caching

Caching HTTP error responses from the Origin Server provides the Web Engine with the ability to validate incoming requests faster and reduce unnecessary access to the Origin Server.

As an example, the Origin Server sends back a response with the status “503 Service Unavailable” and includes the *maximum age* in the response. The Web Engine caches the response locally, and for any subsequent client requests for the same content, the Web Engine compares the cached response age with the maximum age returned in the response. If the cached response is expired, the Web Engine rechecks the Origin Server; otherwise, the Web Engine sends the cached response to the client.

The HTTP response headers must include the max-age, expiry, etag, and other fields that are required to determine whether the responses can be cached. The HTTP response headers that can be cached are those that indicate some error has occurred with respect to the client request (4xx or 5xx status codes).



#### Note

Error response 416 is not cached when the Origin server responds with Transfer-Encoding:Chunked header. Whenever the Origin server sends chunked encoding, whatever status is returned, the response is not cached.

### 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, generate or validate the URL signature, or rewrite or redirect the URL.



#### Note

The following Service Rule actions are supported for the Web Engine: allow, block, rewrite the URL, no cache, redirect the URL, resolve the URL, revalidates cache, and validate the URL signature.

## Windows Media Streaming Engine

The Windows Media Streaming 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 Streaming 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 Streaming engine acts as Windows Media Server for prefetched or cached content stored locally. The request is served by RTSP and HTTP. Windows Media Streaming engine checks with the storage function on the Service Engine to see whether the content is stored locally; if the content is not found, Windows Media Streaming 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 1-18. There are two options:

- Hierarchical Caching Proxy—If content is not found locally, Windows Media Streaming 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 information on cache management for Windows Media Streaming, see the “[Content Manager](#)” section on page 1-7.

### **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, Windows Media Streaming 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 benefiting 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. Windows Media Streaming streams content at a much higher data rate than specified by the stream format. For example, using Fast Cache, Windows Media Streaming 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—which ever 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.

### Caching SDP Files for RTSP Broadcast Live

Live streaming is content that is streamed while it is still being encoded by an encoder. The two kinds of Windows Media live streaming are as follows:

- Playlist live—One or more content items are streamed sequentially.
- Broadcast live—Live and prerecorded content can be streamed to more than one client simultaneously. The SE streams the content to all clients, which does not allow the clients to perform seeks on the stream.

Streaming is accomplished by using HTTP live or RTSP live. HTTP live uses Windows Media Streaming Protocol (MS-WMSP) where the wms-hdr in the WMS-Describe-Response describes the content. RTSP live uses RTSP where the Session Description Protocol (SDP) file in the DESCRIBE response describes the content.

The RTSP playlist live SDP file cannot be cached because the SDP file keeps changing to reflect the different content playlists.

The SDP file for RTSP broadcast live does not change unless the program is stopped, so it can be cached on the streaming SE. Once the SDP file is cached, it can be used to compose the DESCRIBE response. No further requests for the SDP file from the upstream server (SE, Content Acquirer, or Origin server) are necessary.

**Note**

The SDP file cannot be cached if content requires authorization by either the Origin server or the SE.

### 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, Windows Media Streaming 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.

To avoid doing a CAL lookup resolve for each incoming Windows Media Streaming live request, the live hierarchical splitting URL is cached and is then used by all subsequent Windows Media Streaming live requests for the same live program.

**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. Windows Media Streaming can receive and deliver Windows Media content over IP multicast or unicast transmission in the following combinations:

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

Windows Media Streaming 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. Windows Media Streaming 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

Windows Media Streaming 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. Windows Media Streaming 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 Windows Media Streaming checks to see whether the incoming stream is present. If it is, Windows Media Streaming joins the stream and splits it to the new client. If the request is the first client request for this stream, Windows Media Streaming sends the request to the origin server and then serves it to the new client.

### ASX Request Handling

Web Engine generates meta-responses for the following Windows Media Streaming ASX requests:

- Requested Windows Media Streaming asset is prefetched
- Unicast (.asx) request for Windows Media Streaming live program is scheduled
- Multicast (.nsc.asx) request for live program is scheduled

When the **wmt disallowed-client-protocols** command is configured, Web Engine generates the meta-response based on the protocols enabled. When both RTSPU and RTSPT are disabled, only the HTTP URL is generated in the meta-response. However, when HTTP is disabled, the generated ASX file still contains the HTTP URL, so that the content can be served by the Web Engine as a progressive download (as opposed to live streaming by Windows Media Streaming). For .nsc.asx files, only the HTTP URL is generated.

### VOD ASX Request

Web Engine does lookups for incoming ASX requests in the following manner:

- If the ASX asset is cached or prefetched, the asset is served.
- If the ASX asset is not found, Web Engine strips the .asx extension from the URL and performs the lookup again.
  - If the asset is found (after stripping the .asx from the URL), Web Engine generates the meta-response for the requested Windows Media Streaming ASX request.
  - If the asset is not found (after stripping the .asx from the URL), no meta-response is generated and the request is treated as a cache miss.

### Live ASX Request

In the case of a unicast live request or a multicast live request, the Web Engine generates the meta-response for found assets. If the asset is not found, Web Engine generates a “403 Forbidden” error message and sends it to the client.

### NSC Request Handling

An NSC request is a managed live streaming request. When the live program schedule is started, the NSC content is created by Windows Media Streaming.

For Web Engine lookups of NSC files, CAL returns the NSC file location where the content can be served from, or returns “Not in Schedule.”

### Authentication

Windows Media Streaming 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, Windows Media Streaming 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 1-4](#).

**Table 1-4 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.
Outgoing Session Bit Rate	The maximum bit rate per session that can be delivered to a client.

**Table 1-4 Bandwidth Management Capabilities (continued)**

<b>Bandwidth Management</b>	<b>Description</b>
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.

## 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 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. Then, a client session and a server session are created.

- 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 1-18. 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.

For information on cache management for the Movie Streamer, see the “[Content Manager](#)” section on page 1-7.

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.

### 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 Hinter. The linear hinter process can be initiated manually by the administrator or dynamically triggered by the first request for the content.

The Movie Streamer Linear Hinter 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 Internet Streaming 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.

### Authentication

The Movie Streamer Engine supports the Basic authentication mode.

**URL Signing**

For more information see the “[URL Signing](#)” section [on page 1-30](#).

**Flash Media Streaming Engine**

The Flash Media Streaming engine incorporates the Adobe Flash Media Server technology into the VDS-IS 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** Starting with Release 4.0, the Flash Media Server 3.5 is upgraded to Adobe Media Server 5.0.2.

The 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](http://www.adobe.com).



**Note** VDS-IS supports the Adobe Flash Media Server Administration 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 VDS-IS Service Engine. See the “[Configuring Flash Media Streaming—General Settings](#),” [page 4-43](#) 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 VDS-IS or from any upstream Service Engine or origin server. See the “[Web Engine](#)” section [on page 1-17](#) for more information.

**RTMP Requests**

The SWF file is a compiled application that runs on the Adobe Flash Player, and may contain Real Time Media Protocol (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.

Flash Media Streaming also supports RTMPT and RTMPTE on port 80. RTMP Tunneled (RTMPT) encapsulates the RTMP data within HTTP requests to traverse firewalls. RTMP Tunneled Encrypted (RTMPTE) encrypts the communication channel, tunneling over HTTP.

**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/path/foo.flv`

In this format, *rfqdn* is the routing domain name of the Service Router, *vod* 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* 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/path/foo.flv` format for VOD streams, but the SE replaces the *vod* directory with the string specified in the **flash-media-streaming application-virtual-path vod map** command.

Use the **flash-media-streaming application-virtual-path vod 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" directory to "media" for the go-tv-stream.com origin server, use the **flash-media-streaming application-virtual-path vod map media** command.

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" 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. The Flash Media Streaming engine also supports RTMPT and RTMPTE over port 80. 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 1-18. 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 to adapt to changes in network conditions.

Multi-bit rate streaming has the following requirements:

- The origin server must be running Flash Media Server 3.5
- The client must be using Flash Media Player 10 or later
- The encoder for VOD must be running Flash Media Encoder CS4
- The 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.

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” in the path is automatically proxied.

### Unicast Streaming

The Flash Media Streaming engine supports unicast flash streaming.

### URL Signing

Flash Media Streaming supports signed URLs, which adds additional security. The URL signature generation is based on a key that is a shared secret between the component generating the URL signature and the component validating the URL signature. The URL signature can be generated by the Service Engine, another component external to the Service Engine, or the web portal.

For more information about the URL signatures, see the “[Configuring URL Signing Key](#)” section on page 4-27.

## Codecs

Flash Media Streaming supports the On2 VP6 codec, as well as those listed in [Table 1-5](#).

**Table 1-5      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.
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.

## Flash Media Streaming DCSP Marking

Starting with Release 3.3.0, VDS-IS supports per session DSCP marking for Flash Media Streaming including both VOD and Live.

The DSCP value is a 6-bit field in the IP header, which takes any value between 0 and 63. The Delivery Service specific DSCP value shall be set using the AuthSrv Service Rule file. A new XML tag is added in the rules XML file

```
<Rule_Dscp matchGroup="grp1" protocol="rtmp" dscp-bits="10" />
```

The above rule will match the *matchGroup* defined by a regex pattern or domain name and the attribute *dscp-bits* will be applied to the matching pattern. The attribute is the DSCP value ranging from 0 to 63. If the *dscp bits* is not specified in the rules xml file, the default DSCP value i.e., 0 is considered.

Using rule files provides flexibility to apply DSCP values to different matched patterns such as domain name, URL, IP address, and so on. To support DSCP per Delivery Service, you need to configure the Delivery Service domain name in the rule file.



**Note** The FMS per session DSCP marking feature is supported only on IPv4 protocol. The feature is disabled for IPv6 protocol by default.

## 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, VDS-IS creates a connection to the origin server to get the stream. No client information is sent to the origin server.

## Content Delivery System Architecture

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 VDS-IS 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 VDS-IS 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/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.

Flash Media Streaming supports live stream splitting. For more information about live stream splitting, see the [“Live Stream Splitting” section on page 1-23](#).

### Flash Media Streaming Query String

Previously, if an RTMP request had a query string in the URL for VOD, the Web Engine could decide whether or not to cache the content based on the Web Engine configuration. However, if the query string in the RTMP URL included the end-user specific parameters and not the stream name, every request would have a different URL because every user has a different query string. This leads to the same content getting cached multiple times.

The **flash-media-streaming ignore-query-string enable** command tells Flash Media Streaming to remove the query string before forwarding the request to the Web Engine in the case of VOD, or before forwarding the request to the forwarder SE in the case of live streaming.

If URL signature verification is required, the sign verification is performed before the query string check is invoked. The URL signing and validation, which adds its own query string to the URL, continues to work independently of this enhancement.

When the **flash-media-streaming ignore-query-string enable** command is entered, for every request in which the query string has been ignored, a message is written to the FMS error log, and the Query String Bypassed counter is incremented in the output of the **show statistics flash-media-streaming** command. The FMS access log on the edge SE contains the original URL before the query string was removed.

The **flash-media-streaming ignore-query-string enable** command affects every VOD and live streaming request and is not applicable to proxy-style requests.

### 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 VDS-IS.

**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 VDS-IS software on the SE.

VDS-IS 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. The SWF files and associated HTML pages are either prefetched or hosted in the origin server.
2. The client uses a web browser to access the HTML page, which also loads the SWF file.
3. The SWF file is accessed using the SRDN.
4. The Service Router redirects the request to a Service Engine.
5. The SWF file is downloaded to the web browser.
6. The 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. The 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. The 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.

**Note**

URL signing for interactive applications is supported. For more information, see the “[URL Signing and Flash Media Streaming](#)” section on page H-13.

## Service Router

The Service Router has three parts:

- [Request Routing Engine, page 1-34](#)
- [Proximity Engine, page 1-47](#)

The Service Router can be configured as both the Request Routing Engine and the Proximity Engine, or the Service Router can be configured only as the Request Routing Engine. Additionally, the Service Router can act as a standalone Proximity Engine by not configuring the Request Routing Engine as the authoritative DNS server.

The Proximity Engine contains the functionality of the Proximity Servers used for proximity-based routing. See the “[Proximity-Based Routing](#)” section on page 1-41 for more information on this routing method. The Proximity Engine peers with network routers and listens in on route updates to get topology and routing path information. This information is used to locate the closest resource in the network. Real-time measurements of reachability and delay are also considered. See the “[Proximity Engine](#)” section on page 1-47 for more information on the Proximity Engine.

## Request Routing Engine

The *Request Routing Engine* 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 Request Routing Engine 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.

### Routing Redirection

There are three ways for client requests to get routed to the Request Routing Engine and on to the Service Engine:

- Router fully qualified domain name (RFQDN) redirection
- DNS-based redirection
- IP-based redirection

#### RFQDN Redirection

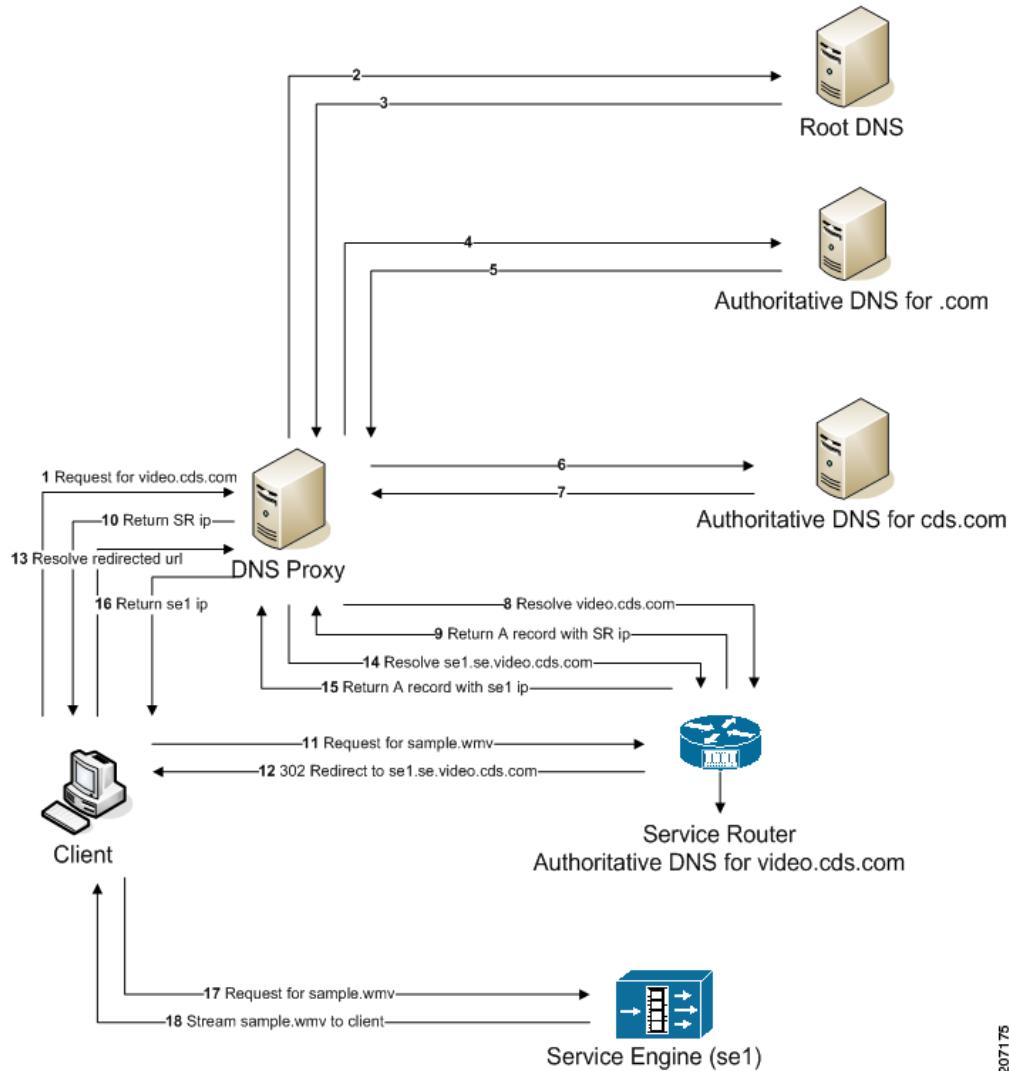
RFQDN redirection is the default configuration. With RFQDN redirection, client requests are resolved to the Request Routing Engine by the DNS server and the Request Routing Engine redirects the request to the Service Engine based on route tables created from the Coverage Zone file and the current load of the Service Engines. The redirected URL is `http://SENAMESE.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://SENAMESE.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 of `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.

### DNS-Based Redirection

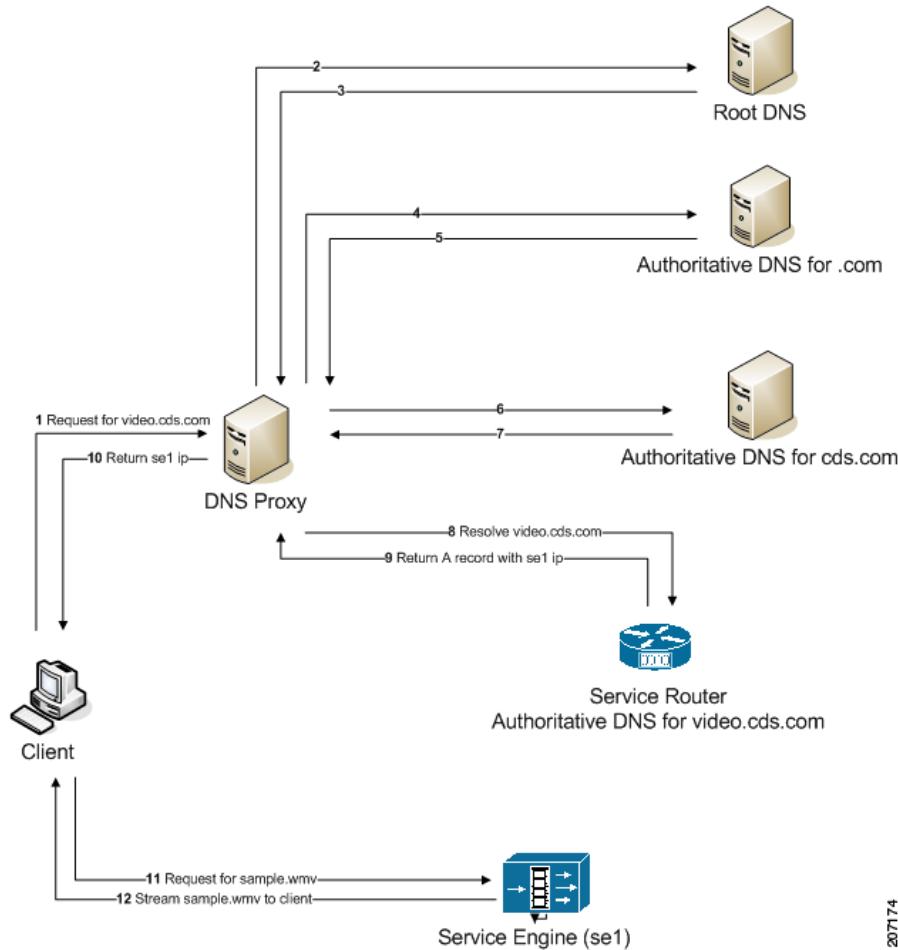
DNS-based redirection enables requests to get directly routed to the Service Engine without any 302 redirects. It also allows content to be streamed without transforming the request URL.



**Note** When DNS-based redirection is used, for application-level requests, last-resort redirection is supported. However, on the DNS plane, an A record with the last-resort domain name or IP address is not returned.

Figure 1-3 describes the Service Router's Request Routing Engine workflow using DNS-based redirection.

**Figure 1-3 Request Routing Engine Workflow with DNS-Based Redirection**



When DNS-based redirection is enabled, the DNS proxy contacts the Request Routing Engine to resolve video.cds.com (step 8 in Figure 1-3), the Request Routing Engine determines which Service Engine to redirect the request to based on load, location, and other heuristics, and directly returns the appropriate Service Engine's IP address instead of the Service Router's IP address. The client then directly requests the content from the Service Engine instead of the Service Router.

**Note**

The TTL for the DNS proxy requests is one second. A one-second TTL ensures that the DNS proxy keeps sending requests to the Request Routing Engine, which in turn causes the Request Routing Engine to determine the best Service Engine at that point in time, and not to redirect the request to the same SE.

**Note**

There are certain side effects in adopting this approach. They are as follows:

- When creating the Coverage Zone file, the IP address of the DNS proxy needs to be used for the client IP address range.
- If proximity-based routing is enabled, it uses the IP address of the DNS proxy in computing the proximity.
- If location-based routing is enabled, the location of the DNS proxy is taken into consideration in the selection of the SE.
- Service-aware routing cannot be used because the protocol and content type are not considered at the DNS level.
- Content-based routing cannot be used because the protocol and content type are not considered at the DNS level.

To configure DNS-based redirection, use the **service-router redirect-mode dns-redirect** command.

```
service-router redirect-mode dns-redirect {all | domain domain}
```

The following example enables DNS-based redirection with the cdsfms.com domain as the domain used to redirect all client requests to:

```
SR(config)# service-router redirect-mode dns-redirect domain cdsfms.com
```

To display information about the redirect mode, use the **show service-router redirect-mode** command.

To display the statistics, use the **show statistics service-router summary** command and the **show statistics se** command. The output for the DNS-Based Redirection feature is listed as DNS Requests. In addition to these two show commands, there is also the **show statistics service-router dns** command.

### IP-Based Redirection

When IP-based redirection is enabled, the Request Routing Engine uses the IP address of the Service Engine in the URL instead of the hostname. The redirected URL is `http://<se ip addr>/ipfwd/<rfqdn>/<path>`. The IP-based redirection method avoids the extra DNS lookup that was required in the RFQDN redirection.

**Note**

The Web Engine does not support IP-based redirection.

### Off-Net and On-Net Clients

The Request Routing Engine chooses the Service Engine based on two scenarios:

- Client is directly connected to the service provider's network (on-net).
- Client is roaming outside the home network (off-net).

When clients are connected to the service provider's network, the Service Engine is chosen based on the requested FQDN, the client's IP address, and the responsiveness of the Service Engine. The Request Routing Engine compares the client's IP address against a table of address ranges representing the client

subnets assigned to each Service Engine. This table is known as the *Coverage Zone file*. The Coverage Zone file provides information on the proximity of the client to the Service Engine based on each client's IP address.

If the client is not connected to the service provider network and location-based routing is enabled, the Request Routing Engine compares the latitude and longitude of each Service Engine, which is defined in the Coverage Zone file, with the latitude and longitude of the client, which is obtained from the Geo-Location servers, to assign a Service Engine that is geographically closest to the client. For more information, see the “[Location-Based Routing](#)” section on page 1-41.

## 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 VDS-IS network.

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.



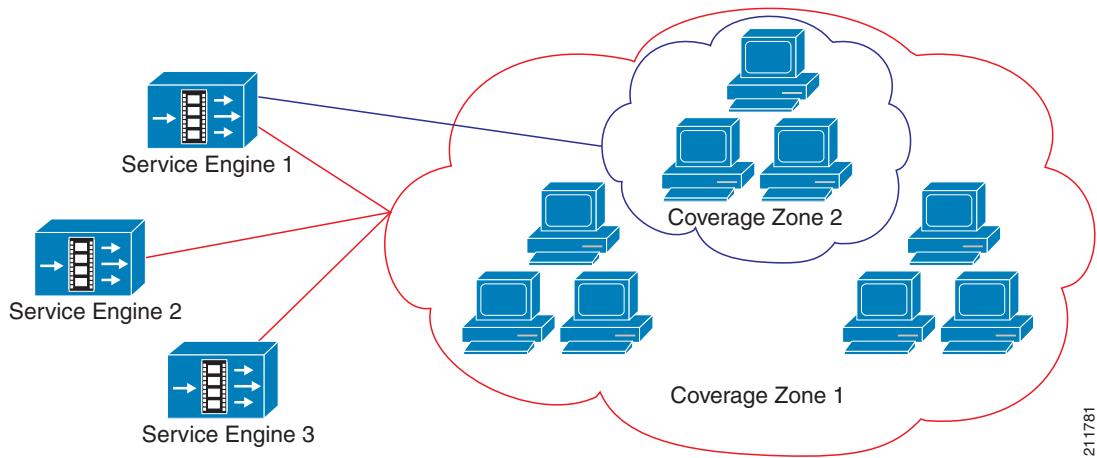
**Note** When DNS-based redirection is enabled, the Coverage Zone file needs to have entries with respect to the IP address of the DNS proxies instead of the client IP address.

If a specific IP address is in multiple coverage zones, the one with the more specific range is selected. If no match is found in the coverage zone data and if location-based routing or proximity-based routing is enabled on the Request Routing Engine, the Request Routing Engine looks up the best Service Engine closest to the client. 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 1-4](#), 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 1-4** Coverage Zone Example



211761

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.

## 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, as defined in the Coverage Zone file.

If the client's subnet is not defined in the Coverage Zone file, the Request Routing Engine checks the following routing methods to see if they are configured:

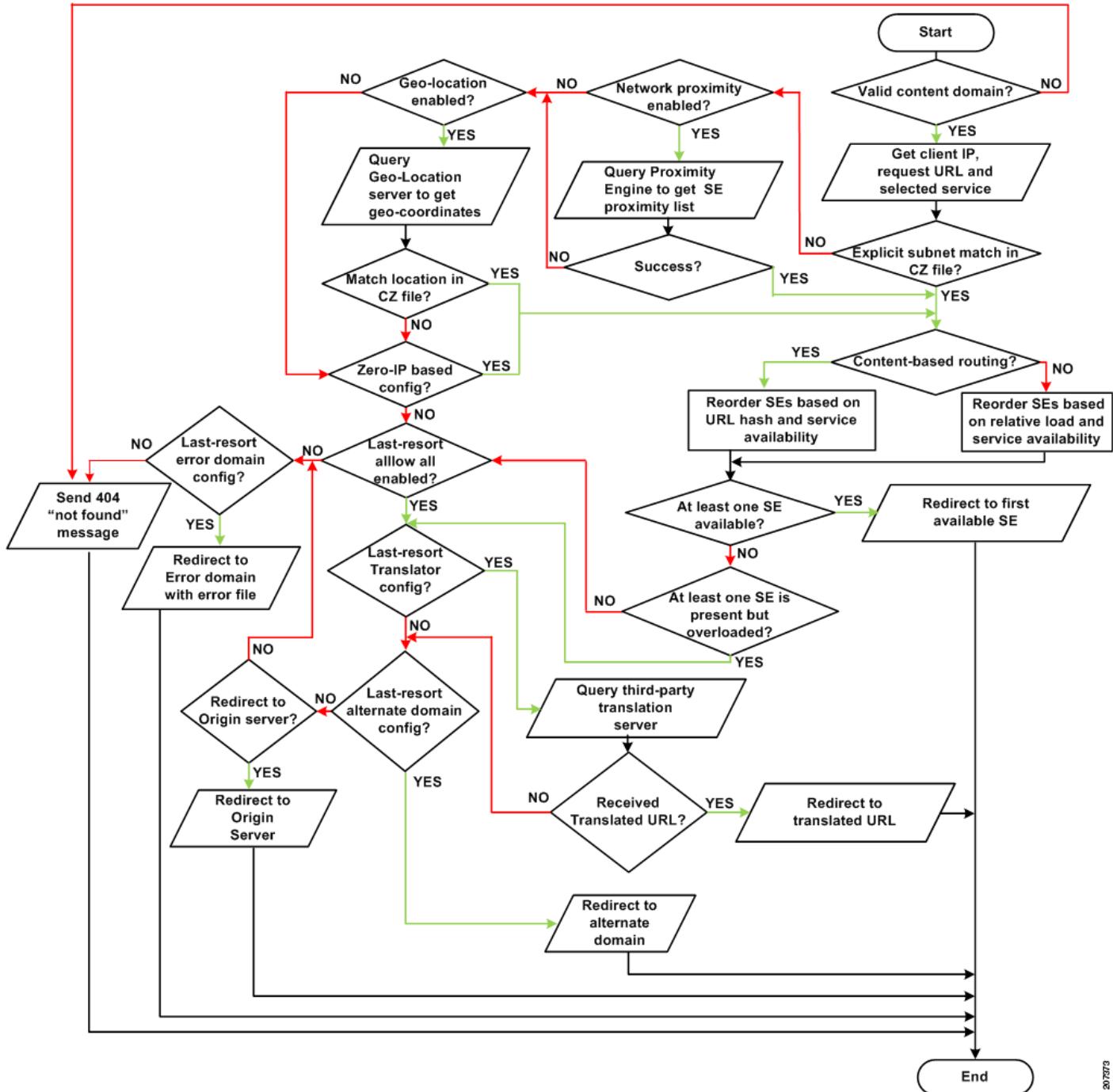
- [Load-Based Routing, page 1-40](#)
- [Proximity-Based Routing, page 1-41](#)
- [Location-Based Routing, page 1-41](#)
- [Zero-IP Based Configuration, page 1-41](#)
- [Last-Resort Routing, page 1-42](#)
- [Service Aware Routing, page 1-43](#)
- [Content-Based Routing, page 1-44](#)



The keepalive messages between the Service Router and Service Engine are transmitted and received on port 2323. However, the software inter-operates 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.

Figure 1-5 describes the order in which the different routing methods are addressed in the Request Routing Engine.

**Figure 1-5 Request Routing Engine Workflow of Routing Methods**



### 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.

**Note**

Bursts of traffic (such as 800 connections per second) may cause the Web Engine to become disabled before it can transmit notification to the SR that the threshold has been reached.

### Proximity-Based Routing

Proximity-based routing offers more intelligence to service routing by using network proximity for Service Engine selection. In proximity-based routing, the Request Routing Engine uses the collocated Proximity Engine, or an external Proximity Server that runs routing protocols to get route updates from network routers. A Proximity Server listens for OSPF, BGP, and IS-IS updates and provides proximity information between clients requesting content and Service Engines that have the requested content. It provides a list of Service Engines to the Request Routing Engine ranked in order of optimal routes for content and messages in a network.

Proximity-based routing is used to select the closest Service Engine for a specified client IP address. The Proximity Engine and Proximity Server communicate with network routers and listen in on route updates and gets topology and routing path information. This information is used to locate the closest resource in the network. Real-time measurements of reachability and delay are also considered.

For information on the collocated Proximity Engine, see the “[Proximity Engine](#)” section on page 1-47.

### Location-Based Routing

Location-based routing is used for off-net clients. Off-net clients are clients that are not directly connected to the service provider network. Location-based routing is designed to work with load-based routing. When both are enabled, the Request Routing Engine first looks up the client IP address in the Coverage Zone file. If there is no subnet match, the client’s geographical location is compared to the geographical location of the Service Engines listed in the Coverage Zone file, and the closest and least-loaded Service Engine is selected. Geographically locating a client is used when users roam outside of their home network.

To provide routing to off-net clients, the Request Routing Engine communicates with a Geo-Location server, which maps IP addresses to a geographic location. For redundancy, the CDSM can be configured with a primary and secondary Geo-Location server.

The Geo-Location server identifies the geographical location of an off-net client by the latitude and longitude of the client. The Request Routing Engine compares the client’s location with the location of the Service Engines participating in that Delivery Service and chooses the best Service Engine to serve the content.

### Zero-IP Based Configuration

The zero-ip based configuration is a catch-all condition for routing. It can be used in combination with proximity-based routing and location-based routing. If an SE cannot be found through location-based routing or proximity-based routing, the zero-ip based configuration is taken into account for selecting an SE.

The zero-ip based configuration 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.

### 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 or translator response 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 (for location-based routing) listed in the Coverage Zone file.



**Note** When DNS-based redirection is used, for application-level requests, last-resort redirection is supported. However, on the DNS plane, an A record with the last-resort domain name or IP address is not returned.

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.

Last-resort routing allows redirecting a request to an alternate domain or Origin server (if Enable Origin Server Redirect is enabled) for one of the following conditions:

- All SEs in the Delivery Service have exceeded their thresholds
- All SEs in the Delivery Service are unavailable or no SEs are assigned to the Delivery Service
- The client is unknown

Redirecting to the Origin server is allowed if the Enable Origin Server Redirect field is enabled for the content origin. The default setting is enabled. For more information on this configuration parameter, see the “Content Origins” section on page 5-1.



**Note** Unknown clients are only redirected to the alternate domain (last-resort domain) or translator response 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.

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

Last-resort routing could also be configured to redirect a client to an error domain and filename.

The URL translator provides a way to dynamically translate the client request URL to redirect the client to a different CDN. With the URL translator option, the following occurs if the SR uses last-resort routing for a client request:

1. The SR contacts the third-party URL translator through the Web Service API. The Web Service API is described in the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 API Guide*.
2. The third-party URL translator sends the translated URL in the response to the SR.
3. The SR sends a 302 redirect message to the client with the translated URL it received from the third-party URL translator.

The timeout for connecting to the URL translator server is 500 milliseconds. There are no retries if the URL translator cannot be reached.

If there is no configuration on the URL translator for the requested domain or the connection timeout threshold has been reached, the SR last-resort routing falls back to the alternate domain configuration.

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

URL translator last-resort routing supports RTSP and HTTP client requests. For Flash Media Streaming clients (RTMP), the client must be able to handle redirects to a different application name. Most Flash clients cannot support a stream name change; so the filename returned by the translator is ignored.

### 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 4-83](#) 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
- RealOne player
- RealMedia player



#### Note

In addition to redirecting requests based on the user agents listed in this section, requests for content with the following file extensions are served by Windows Media Engine (both HTTP and RTSP requests):

- wma
- wmv
- asf
- asx

Requests for content with the following file extensions are served by the Movie Streamer Engine:

- 3gp
- 3gp2
- mov
- mp4

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** If the Web Engine is disabled on the Service Engine, the Service Engine does not get selected for serving any requests, including Windows Media Streaming, Flash Media Streaming, and Movie Streamer.



**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. If the same SE is not available, requests are routed to the next best SE. If the original SE is available again, requests are routed back to it irrespective of the number of interim redirects to the second best SE.

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.



**Note** Content-based routing does not work with clients sending signed URL requests. The hashing algorithm for content-based routing considers the whole signed URL, so a signed URL request for the same content may be redirected to a different SE.

## Request Routing Engine Workflow of Coverage Zone, Proximity-Based Routing, and Location-Based Routing

The Request Routing Engine workflow for clients connected to the service provider's 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.

If the Request Routing Engine does not find the client's subnet in the Coverage Zone file and proximity-based routing has been enabled, the following occurs:

- a. The Request Routing Engine communicates with the Proximity Engine and gets the SE proximity list with the SEs that have the least network cost listed first.
- b. The Request Routing Engine selects the closest Service Engine for the specified client IP address.
- c. The Request Routing Engine performs a protocol-specific redirection with the closest Service Engine.
- d. The client issues an HTTP, RTMP, or RTSP request to the Service Engine.
- e. The Service Engine serves the content.

If the Request Routing Engine does not find the client's subnet in the Coverage Zone file and location-based routing has been enabled, the following occurs:

- a. The Request Routing Engine communicates with a Geo-Location server and gets the geographical coordinates of the client's IP address.
- b. The distance is calculated between the client and the Service Engines, and the Service Engine closest to the client is selected.
- c. The Request Routing Engine performs a protocol-specific redirection with the closest Service Engine.
- d. The client issues an HTTP, RTMP, or RTSP request to the Service Engine.
- e. 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 of the registered devices. The Service Engine sends a keepalive 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 VDS-IS 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

The Request Routing Engine supports the following redirections:

- **HTTP ASX Redirection** Used if the requested file has an.aspx 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 4-122.
- **HTTP 302 Redirection** Used if the protocol is HTTP and the file extension is not .asx. This is the native HTTP redirection.
- **RTSP 302 Redirection** Used if the protocol is RTSP and the client is QuickTime or Windows Media. This is the native RTSP redirection.
- **RTMP 302 Redirection** Used if the protocol is RTMP and the client is Adobe Flash Player, Adobe Media Player, or Adobe Flash Lite Player.

Normal requests for files with an .asx extension returns a status 200, unless HTTP 302 redirection is enabled.

## 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 VDS-IS), 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/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 VDS-IS, 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

The Cross-Domain Policy feature can be enabled through the CDSM. See the “[Configuring Cross-Domain Policy](#)” section on page 4-110 for more information.

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.

## Unified Routing Table

The unified routing table uses one global route context for all domains, with all SEs from the Coverage Zone file added to one set of route tables. This is a good option if the VDS-IS serves a number of different domains (configured as delivery services), but uses the same set of SEs for the different delivery services (domains). By enabling the unified routing table in this scenario, the memory usage on the SR is reduced.

If the VDS-IS is configured with fewer domains or the SEs are not all serving the same domains, then the memory usage is not impacted as much, and not enabling unified routing may be a better option.

The unified routing table option is disabled by default. To enable unified routing on the SR, enter the **service-router unified-routing -table enable** command.

**Note**

Not enabling the unified routing table increases the memory usage on the SR. Make sure the memory usage does not exceed the recommended limit, which is 1.5 GB when the SR is running with a load and no configuration changes are occurring.

## Proximity Engine

The Proximity Engine leverages routing information databases (IGP and BGP) by interconnecting and peering with routers. This information is used to compute the network distance between a source address, referred to as the proximity source address (PSA) and a target address, referred to as the proximity target address (PTA). This distance is known as the *proximity rating of the PTA*.

The Proximity Engine is configured as one of the Proximity Servers for the proximity-based routing method. See the “[Proximity-Based Routing](#)” section on page 1-41 for more information.

**Note**

The Proximity Engine only participates in the Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Border Gateway Protocol (BGP) to gather information to make proximity decisions. The Proximity Engine is not a router and does not ever use the information to route traffic.



**Note** The Proximity Engine is only supported on the CDE205 and the CDE220-2G2 platforms.

The standby interface is not supported for Proximity Engine. Use port channel configuration instead.

The Proximity Engine operates in an IP routing domain where the Interior Gateway Protocol (IGP) or BGP is used to distribute routing information across the domain. For the proximity function to work, at least one of the following is required:

- Enabled link-state protocol, such as OSPF or IS-IS for IGP proximity, which is required if the Proximity Engine is going to peer with IGP routers.
- Enabled policy routing protocol, such as BGP for best-path proximity and location-community proximity, which is required if the Proximity Engine is going to peer with BGP routers.



**Note** All BGP routes must resolve to IGP next hops or directly connected routes.

Routers running OSPF or IS-IS establish adjacencies with their directly connected neighbors and exchange their connectivity view (that is, each router advertises its visibility about its adjacencies). Advertisements are flooded throughout the whole routing area and each router stores each received advertisement in a link-state database (LSDB).

The LSDB contains the topology of the whole network and each router uses it to compute the Shortest Path Tree and the Routing Information Base (RIB) that contains each known IP prefix in the network and its corresponding next-hop.

OSPF and IS-IS are the two IP link-state protocols. They operate quite similarly:

- Establish adjacencies with directly connected neighbors
- Create a routing update packet (OSPF LSA and ISIS LSP) containing the router connectivity
- Flood routing updates (LSA or LSP) throughout the routing area
- Collect all received routing updates in a LSDB
- Compute shortest first path (SPF) algorithm
- Populate the RIB with the result of SPF

The difference between OSPF and IS-IS is in the way packets are formatted and exchanged (encapsulation) and in the way adjacencies and flooding are handled over broadcast media. From a routing computation perspective, both protocols behave the same and therefore the Proximity Engine operates the same in networks deploying OSPF or ISIS.

The Proximity Engine makes proximity decisions using information from the same link-state database that is passed between routers using OSPF or IS-IS. For these reasons, the Proximity Engine must be configured to make either OSPF or IS-IS adjacencies to gather link-state database information for routers in the same autonomous system, and BGP adjacencies to gather the BGP routing information for routers in the different autonomous systems.

## Proximity Engine Request Flow

Following is the Proximity Engine request flow:

1. The Request Routing Engine sends the proximity request to the Proximity Servers, the first of which could be the collocated Proximity Engine.

The proximity request specifies a PSA (the client's IP address) and a set of one or more PTAs (IP addresses of the SEs).

2. The Proximity Engine receives the proximity request and performs a route lookup on the PSA.
3. The Proximity Engine determines whether the request should be handled by IGP, BGP, or locally. Local routing is used when both the PSA and PTA are both local to the network. If the proximity algorithm for BGP location community is enabled, and the PSA has community attribute information, then both BGP and IGP routing information is considered.

The Proximity function takes into account:

- Routing topology
- Inter-autonomous system reachability
- Optimal path taken by the requested data

4. The Proximity Engine sends the response back to the Request Routing Engine.

In the proximity response, the Proximity Engine returns a list of proximity target addresses and the cost associated with each address. This list includes all of the IP addresses of all of the SEs registered to the CDSM. Using the proximity response data, the Request Routing Engine can select the closest (best) target.



**Note** If multi-port support is configured on the with multiple IP addresses, only one valid IP address of that SE is included in the list. If this is selected, it can load balance the requests among the streaming interfaces.

### Proximity Ranking

The proximity ranking could include the following proximity algorithms:

1. BGP community-based proximity
2. BGP best-path proximity
3. IGP proximity

The first two algorithms are only used if they are enabled. The last one, IGP proximity, is enabled when an IGP is configured.

The proximity ranking always contains the proximity target list (PTL) addresses in the same order as above. For example, if there is a PSA and two PTAs (PTA1 and PTA2), and all proximity algorithms are enabled, the following rules are applied:

1. If PSA and PTA1 have at least one community in common and PTA2 does not have a common community, PTA1 is preferred over PTA2.
2. If both PTA1 and PTA2 have at least one community in common as the PSA, the next weight is considered.

The larger the number, the more weight the community has. If PTA1 has a weight of 5 and PTA2 has a weight of 2, PTA1 is preferred over PTA2.

3. If both PTA1 and PTA2 have the same weight, the next algorithm is considered, which is BGP best-path.
4. For BGP best-path, the PTA with the smallest AS-hop count is preferred. If both PTAs have the same AS-hop count, the next and final algorithm is considered, which is IGP proximity.
5. For IGP proximity, the PTA with the lowest IGP metric is preferred.

## BGP Proximity Algorithms

### Community-Based Proximity

Two distinct proximity algorithms are used:

- IGP-proximity algorithm gives an ordered list of SE IP addresses known in the IGP database (OSPF or IS-IS).
- BGP-proximity algorithm gives an ordered list of SE IP addresses known in the BGP table.

While the combination of the IGP and BGP basic proximity is sufficient for the proximity calculation for most network deployments, they may not be appropriate for some network deployments, such as a Multiprotocol Label Switching (MPLS) network. Most of the time it is sufficient to rank the prefixes and make the recommendation for the prefixes based on whether the PSA and the PTA are in the same rack (the most preferred ranking), the same point of presence (POP), the same city, or the same autonomous system (AS) (the least preferred).

When the BGP community-based proximity option is enabled, additional location information is included in the proximity calculation to influence application-level traffic optimization in the network. When the community-based proximity option is not used, the proximity request is handled by IGP proximity.

The BGP community-based proximity requires that the PSA has a BGP community string. PTAs that have the same BGP community string as the PSA are ranked as more preferred than PTAs that do not have the same BGP community string as the PSA. The association of PSA and PTA community attributes is configurable by specifying the target (PTA) community values to association with the location (PSA) community, and optionally assigning a preference level. For more information, see the “[Configuring the BGP Community-based Proximity Settings](#)” section on page 4-118. For the remaining PTAs that have different community strings, they are ranked by IGP proximity.

### Best-Path Proximity



**Note**

Best-Path proximity algorithm requires the configuration of the BGP proximity settings.

When the BGP best-path proximity option is enabled, the BGP best-path algorithm ranks each route included in the PTA based on the attribute values associated with each route.

### Redirect Proximity



**Note**

Redirect proximity algorithm requires the configuration of the SRP and the BGP proximity settings.

If the PSA is learned from another AS, the current Proximity Engine does not have the best knowledge to handle the request. In this case, if the BGP redirect proximity option is enabled, the Proximity Engine sends back a Redirect response to the Service Router. The Redirect response contains the list of Proximity Engines that reside in the same AS as the PSA. The Service Router then sends the proximity request to one of these Proximity Engines.

## Service Routing Protocol

The Service Routing Protocol (SRP) uses distributed hash table (DHT) technology to form a distributed network of Proximity Engines. SRP is highly scalable and resilient. SRP is implemented as an overlay network on top of IPv4 or IPv6 transport. Currently, only IPv4 is supported.

**Note**

SRP is required if the Redirect proximity algorithm is enabled. SRP is used to gather and store information about all of the Proximity Engines that are available for redirection.

A *DHT network* is a logical network composed of Proximity Engines that have the same DHT domain. Although DHT does not play any direct role in responding to the proximity service, it is the integral part of the Proximity Engine system that gathers and stores information about other Proximity Engines in the network to form a cohesive, resilient proximity service network.

## Content Delivery System Manager

The Internet Streaming Content Delivery System Manager (CDSM) is a web browser-based user interface. The Internet Streaming CDSM allows the administrator to configure, manage, and monitor delivery services and devices in the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS). Application programming interfaces (APIs) are provided for backoffice integration with the Internet Streaming CDSM.

### Authentication, Authorization, and Accounting

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

User accounts and groups can be added to the Internet Streaming 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 and TACACS+ servers when available, otherwise the Internet Streaming CDSM provides its own authentication server.

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

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

### Device Management

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

## Higher Storage Utilization of VDS-IS

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 VDS-IS 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 Internet Streaming CDSM provides the configuration and monitoring of delivery services, which defines how content is ingested, stored, cached, and published. The Internet Streaming 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 Internet Streaming 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

A VDS-IS that is designed with full redundancy and no single point of failure includes redundant Internet Streaming CDSMs and Service Routers. The redundancy mechanisms for the Content Acquirer and Internet Streamer applications running on the Service Engines operate differently.

### 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.

## Internet Streamer Redundancy

If a Service Engine running the Internet Streamer application fails, the Service Router stops receiving keepalive 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 VDS-IS network is designed with multiple Service Routers, all Service Routers are aware of all Service Engines in the VDS-IS. The DNS servers must be configured with multiple Service Routers and the failover is handled by the DNS servers.

## Internet Streaming CDSM Redundancy

The Internet Streaming 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 VDS-IS network; however, you can have any number of Internet Streaming 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 Internet Streaming CDSM design principle is that the management device is never in the service delivery path. When the CDSM fails, the rest of the VDS-IS 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 VDS-IS. 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 CDSM to a Primary CDSM” section on page 3-12](#).

**Content Delivery System Architecture**



## Network Design

Provisioning the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS) consists of two stages:

- Register the devices to the Internet Streaming Content Delivery System Manager (CDSM) and define the network topology and device groups.
- Configure the delivery services that deliver content to the clients.

This chapter describes the details of the two stages of provisioning a VDS-IS network, how the metadata and the content flows through the VDS-IS, and the features that determine your network design.

- [VDS-IS Topology, page 2-1](#)
- [Delivery Service, page 2-3](#)
- [Content Replication Using a Multicast Cloud, page 2-12](#)
- [Service Workflow, page 2-18](#)
- [Programs, page 2-20](#)
- [IPv6 Support for Client Interfaces, page 2-21](#)
- [HTTPS Settings, page 2-25](#)
- [Wholesale CDN, page 2-30](#)



To achieve the best throughput, we recommend that you configure port channels for the Gigabit Ethernet interfaces. For more information, see the [“Configuring Port Channel” section on page I-6](#).

## VDS-IS Topology

In the VDS-IS topology, the Service Engines are grouped together into locations, such that a Location Tree is a set of locations organized in the form of a tree. The Location Tree represents the network topology configuration that is based on parent-child relationships. The 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.

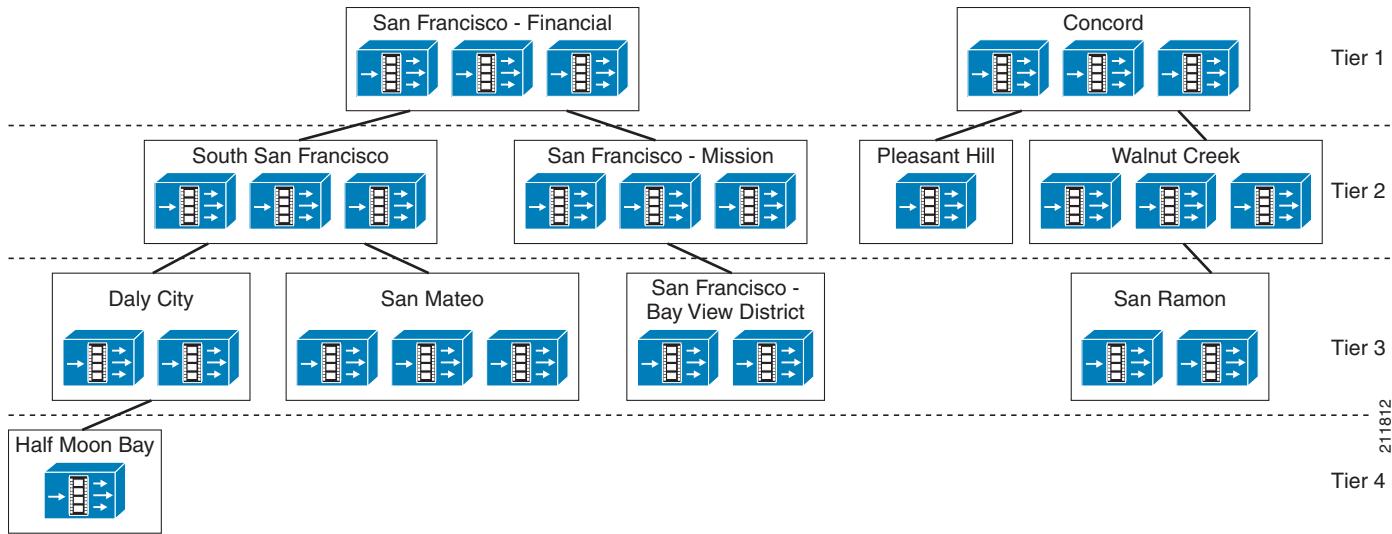
Locations are also classified into tiers. Each tier consists of locations belonging to the same tier. All locations with no parents belong to Tier 1. All locations that are children of Tier 1 locations belong to Tier 2.

**VDS-IS Topology**

The VDS-IS topology can consist of one or more topological Location Trees. A VDS-IS 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 Internet or backbone. Tier 1 locations can communicate with all other Tier 1 locations.



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

The VDS-IS 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 VDS-IS 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 of 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 is a special type of device group that 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.

## 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 collocated at the root location).

## 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 2-5.

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.

## 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.

### 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.

**Delivery Service**

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 VDS-IS 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 the following occurs:
  - It subscribes to the Delivery Service, location A is “closer” to the root location of the Delivery Service than location B
  - 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 “[VDS-IS Topology](#)” section on page 2-1.

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 VDS-IS. Using the combination of the overall topology configuration and the assignment of SEs to delivery services, the VDS-IS 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

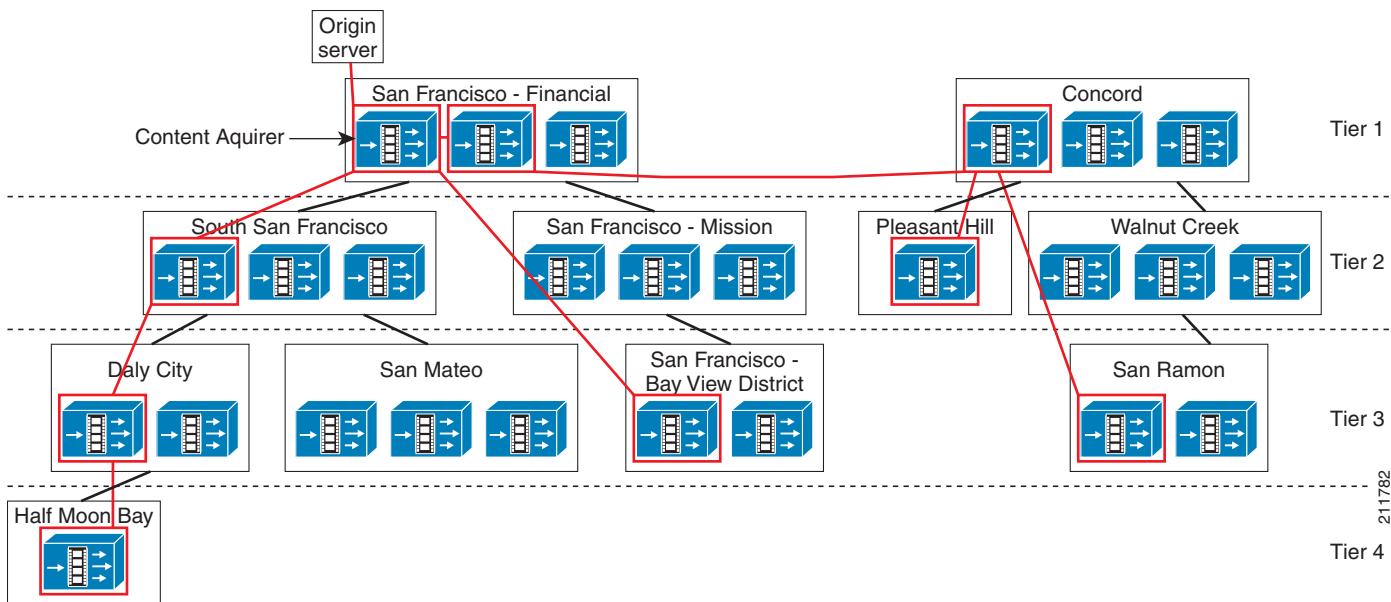
Delivery Services form logical routes for content to travel from an origin server through the Content Acquirer to all of the Service Engines in the Delivery Service. Logical routes for content distribution are based on the device location hierarchy or Location Tree.

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*



211782  
Tier 4

## Types of Delivery Services

The Cisco VDS-IS supports two types of Delivery Services:

- 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 used to manage 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 Internet Streaming CDSM.

The Internet Streaming CDSM provides a user-friendly interface for adding content and configuring crawl tasks. All entries are validated and a Manifest file is generated. The Internet Streaming 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, page 2-9](#)
- [Manifest File, page 2-10](#)
- [Content Acquirer, page 2-11](#)
- [Internet Streamer, page 2-11](#)

## 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 Internet Streaming 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 for the VDS-IS to be able to ingest content:

- HTTP
- HTTPS
- FTP
- CIFS
- SMB

Content can also originate from a local file on the VDS-IS.

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 that all the 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 Internet Streaming 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.

## Origin Server Failover

The Content Acquirer can failover to an alternate Origin server if the primary Origin server fails. The alternate Origin server is configured in the **Services > Service Definition > Content Origins > Failover Settings** page in the CDSM GUI. The Content Acquirer detects Origin Server failure using timeout or other mechanisms. When an Origin Server failure is detected, an alarm is generated to CDSM. The alarm is cleared automatically after a configurable period of time. Meanwhile, the Content Acquirer switches to the secondary Origin Server seamlessly. When all of the Origin Server fails, a 504 response will be generated and sent to client. The operator then manually switches working server among primary OS and any alternate OS. Transaction logs are generated to log these events.

## 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, FTP, 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.

In FTP acquisition, the crawler crawls the folder hierarchy rather than parsing the HTML file. Content ingest from an SMB server for crawl jobs is similar to FTP ingest; that is, the crawler 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 VDS-IS 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 Servers

The no-cache directive in an HTTP server response header tells the client that the content requested is not cacheable. When an HTTP 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.

## Internet Streamer

The Internet Streamer application on the Service Engine participates in the Delivery Service by distributing content within the VDS-IS and delivering content to the clients. The Service Engines can be shared among other delivery services.

### HTTP 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 downloads on a Delivery Service. When HTTP download is disabled, the Web Engine returns a 403 forbidden message. For configuration information, see the “[Creating Delivery Service](#)” section on page 5-16.

# Content Replication Using a Multicast Cloud

The Multicast Cloud feature is a group of multicast-enabled SEs configured to communicate multicast session information with one another. The Multicast Cloud feature is described in the following sections:

- [Introduction to Multicast Cloud, page 2-12](#)
- [Distributing Content Through Replication, page 2-13](#)
- [Configuring Multicast Distribution, page 2-14](#)
- [Multicast Forward Error Correction and Proactive Forward Error Correction, page 2-15](#)
- [APIs for Multicast Cloud, page 2-18](#)



**Note**

The Multicast Cloud feature is supported in all releases starting with Release 3.1.1.

## Introduction to Multicast Cloud

Content is forwarded (or replicated) either by unicast pull (transmission initiated by a client request for the content) or, if it is enabled, by multicast push (transmission initiated in accordance with a preconfigured program or schedule). Unicast content forwarding involves communication between a single sender and single receiver, whereas multicast replication involves communication between a single sender and a selected group of receivers.

Multicasting allows efficient distribution of content to multiple SEs and is useful when many end users are interested in the same content. VDS-IS software supports Pragmatic General Multicast (PGM)-based multicast replication, using either satellite or multicast-enabled terrestrial infrastructures. (PGM is a reliable multicast protocol that enables PGM receivers to report loss of data and request retransmission by the PGM sender.)

In VDS-IS software, the administrator configures the VDS-IS network for multicasting by configuring a Multicast Cloud in the CDSM GUI. The Multicast Cloud consists of one sender SE, an optional backup sender for multicast-to-multicast failover, and at least one receiver SE. All the SEs in one cloud share a unique advertising address, allowing them to communicate multicast session information. SEs that are assigned to the Multicast Cloud must be enabled for multicasting. The Multicast Cloud is then associated with one or more multicast-enabled delivery services. The multicast-enabled SEs assigned to the Multicast Cloud are also assigned to the multicast-enabled Delivery Service.

The SEs that are receivers get their content from the multicast addresses associated with the cloud. The Multicast Cloud is an overlay topology on the location-based distribution tree structure. The clouds can be chained by making a receiver of one cloud the sender of another cloud. For best performance, the SEs in a Multicast Cloud should all be able to receive data at about the same rate. The slowest receiver determines the rate at which the sender pushes the files.

When configuring the Multicast Cloud, the administrator specifies a range of addresses by entering a start IP address and an end IP address. Once a Multicast Cloud is configured, the multicast address range is used to provide each Delivery Service associated with it a unique data Delivery Service multicast address. When a Multicast Cloud is assigned to a Delivery Service, an unused IP address is automatically selected from this range to ensure that the address is used by only one Delivery Service and by only one Multicast Cloud. Because different multicast clouds may be associated with the same Delivery Service, the multicast address used for each Delivery Service needs to be different in each Multicast Cloud.

## Distributing Content Through Replication

After content is acquired from the Origin server by the Content Acquirer of a Delivery Service, it can be replicated through the Delivery Service either by unicast or multicast transmission.

The Delivery Service configuration offers content replication options:

- Multicast and unicast (multicast with failover to unicast)
- Multicast-only
- Unicast-only

### Unicast Replication

The basic Delivery Service distribution architecture provides for unicast content replication using a hop-by-hop, store-and-forward methodology with the forwarder SEs systematically selected on the basis of the manually configured location hierarchy.

To distribute content through unicast, the VDS-IS network automatically creates a unidirectional distribution tree for each Delivery Service. The root node of the tree is the Content Acquirer of the Delivery Service, and each SE subscribed to the Delivery Service is a node on the tree.

For each node, its parent node is also called its forwarder SE. The algorithm for automatically designating the forwarder SE is called the channel routing algorithm.

Three general rules in the current channel routing algorithm are as follows:

1. In each location for each Delivery Service, only one SE fetches content from another location for that Delivery Service. We call this SE the location leader of the Delivery Service. All other SEs in this location use the location leader as the forwarder for this Delivery Service. There can be only one location leader per Delivery Service per location. Note that within one location, different delivery services may have different location leaders.

The location leader is computed automatically by the channel routing algorithm.

Use the **show distribution delivery-service** command to see which SE is the current forwarder for a Delivery Service. The reason/status field in the command output shows why an SE is unable to find a forwarder. Use the **show distribution forwarder-list** command to see the forwarder selection order of an SE for a Delivery Service.

2. The location leader finds a subscribed SE from the closest location on the path toward the Content Acquirer as its forwarder. If all of the potential forwarders in a parent location are down (or unreachable) the location leader skips to the next location level in the hierarchy (towards the Content Acquirer location) to find a forwarder.
3. If the location leader SE fails for some time, another SE in the location takes over as the location leader. If the Content Acquirer fails, another SE in the location takes over as the temporary Content Acquirer.

### Multicast Replication

In multicast content distribution, the sender SE in a Multicast Cloud proactively pushes content into the cloud according to a preconfigured schedule.

The receiver SEs listen on the advertisement IP address for information on content to be replicated from the sender, and then the receiver SEs decide whether or not to accept an advertisement and receive the corresponding content.

## Content Replication Using a Multicast Cloud

Content metadata must be distributed to a receiver first before the content itself can be replicated. Content metadata helps to define what content to retrieve, how content will be retrieved, how recently content has been updated, how content is to be pre-positioned (for example, expiration time), and so on. Metadata is always distributed using unicast. Content, however, can be replicated using either multicast or unicast. A multicast receiver rejects the multicast sender's advertisement of a file if the proper content metadata has not yet arrived.

### Multicast and Unicast



**Note** When a Delivery Service is configured for multicast and unicast, the receiver SE uses unicast to download content only after all carousel passes have been exhausted and after the preconfigured multicast transmission fails. In a Multicast Cloud configuration that uses a backup sender, when the Delivery Service is enabled for multicast and unicast, the failover to unicast occurs when the current active multicast sender has exhausted all of the carousel passes for the file. When there is multicast transmission error or if the receiver edge streamer fails to get the intended content via multicast then the edge streamer will fall back to unicast distribution only after all carousel passes have been exhausted.

If the administrator wants the SEs to fall back to unicast (for example, with a multi-tier unicast deployment using a terrestrial multicast medium), the Multicast Cloud should be configured for a low number of carousel passes (such as 1, 2, or 3).

### Multicast Only

If only multicast replication is desired (for example, with a hub and spoke or star topology deployment using a satellite multicast medium), the Delivery Services should be configured as multicast-only, with a high number of carousel passes configured in the Multicast Cloud (such as 10 or more).

When a Delivery Service is configured to be multicast only (that is, when the delivery services are associated with a Multicast Cloud and the subscribing receiver SE has multicast service enabled), content replication takes place only through multicasting. No retransmission takes place in unicast at all. This prevents background unicast polls from happening and taking up bandwidth. However, if an SE in the multicast-only Delivery Service is not enabled for multicasting, it can continue to request all of the content from a multicast-only Delivery Service through unicasting.



**Note** When the Delivery service is configured as Multicast Only, unicast distribution will not happen if either the multicast network connectivity fails in network or if the sender process fails in sender. The unicast distribution happens only if the multicast receiver process has failed or the receiver process is explicitly disabled by the administrator.

## Configuring Multicast Distribution

To configure the VDS-IS for multicast replication of content, the following tasks need to be performed:

1. [Enabling SEs for Multicasting, page 4-20](#)
2. [Creating Multicast Clouds, page 5-8](#)
3. [Assigning SEs to a Multicast Cloud, page 5-12](#)
4. [Assigning Multicast Clouds to Delivery Services, page 5-14](#)

5. Assigning SE members of the Multicast Cloud to the Delivery Service (**Services > Service Definition > Delivery Services > Assign Service Engines**)

### Multicast Logging Enhancements

The VDS-IS includes enhanced multicast logging to identify the receiver SE that is sending the retransmission requests (NACKs) and to identify why a file is scheduled for multicasting. These logging enhancements provide the following details:

- Any NACKs that are received by the multicast sender SE are logged at the trace level in the dist-meta-sender error log on the multicast sender SE.
- Any NACKs that are related to preparing a file for scheduling are logged in the transaction log.
- Any file that is scheduled for multicasting has the details about why it was scheduled for multicasting. You can obtain the details from the time-based queue or the priority-based queue.

## Multicast Forward Error Correction and Proactive Forward Error Correction

Forward error correction (FEC) is a type of data encoding that protects transmissions against errors, without requiring retransmission. The FEC number denotes the number of packets that is encoded into one FEC transmission group. When the FEC number goes up, the transmission group becomes larger, so the multicast may be more error-resistant. However, there is more computational and bandwidth overhead on the multicast sender and receivers.

Starting with Release 3.2.3, VDS-IS supports assigning FEC value at Delivery Service level via **Services > Service Definition > Delivery Services > Assign Multicast Cloud** page in CDSM GUI.

The FEC default value is 16. If the multicast sender device is a high-end SE model such as a CDE250, you can set this number higher to improve multicast reliability, especially when your network connectivity has a high uniform loss rate. However, we do not recommend that you set this number beyond 64 because it may place too much of a load on all of the receiver SEs.

Starting with Release 3.3.1, VDS-IS supports to configure the FEC proactive parity size, and the FEC proactive delay in the Multicast Cloud configuration and when assigning a Delivery Service to a Multicast Cloud. See the “[Creating Multicast Clouds](#)” section on [page 5-8](#) for more information.

Proactive FEC is the number of extra packets that the multicast sender proactively sends out for every FEC number of data packets. The proactive FEC default value is 0. You can set it higher for better multicast reliability; for example, 2 proactive packets for every 16 FEC packets, at the expense of 12.5 percent traffic overhead (2 divided by 16).

Proactive FEC is an additional reliability measure above and beyond that of normal FEC. Although normal FEC does not incur bandwidth overhead, proactive FEC does. Proactive FEC primarily protects the multicast from uniform losses. For example, if the network has a uniform loss rate of 15 percent, then a proactive FEC of 2 extra packets for every 16 FEC packets (a 12.5 percent bandwidth overhead) cuts the effective loss rate down to 2.5 percent. Most network losses are not completely uniform. Still, during bursts, proactive FEC similarly undercuts the effective burst loss rate. For example, if the burst loss rate is 20 percent while the average loss rate is 2 percent, with proactive FEC at 12.5 percent, the receiver SEs experience a burst loss rate of 7.5 percent and an average loss rate near 0 percent.

## Configuring PGM and File Transmission Parameters Using Multicast Expert Mode

PGM is a reliable multicast protocol defined in IETF RFC 3208. It is designed for applications that require ordered or unordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers. Support for reliable multicasting and file transmission is provided by the

TIBCOsmartPGM FX tool set, which is integrated with the Cisco VDS-IS software. You can configure some PGM and file transmission (FX) parameters through the CDSM GUI, such as the advertisement IP address, multicast-out bandwidth, TTL, FEC transmission group, and so forth.

In some cases, expert users might want to change other PGM and FX parameters to make the multicast file transfer more robust and efficient for their multicast environment. The VDS-IS allows you to change the configuration parameters of the TIBCOsmartPGM FX configuration file manually by using multicast expert mode on the SE.


**Caution**


---

We do not recommend that you change the TIBCOsmartPGM FX configuration file unless you are an expert in PGM multicasting and know how to adjust the configuration parameters.

---

The VDS-IS software contains default TIBCOsmartPGM FX configuration files for multicast sender and receiver SEs. The multicast sender and receiver SEs determine the medium (terrestrial or satellite) being used for the multicast by checking the configuration of the Multicast Cloud, then they read the configuration parameter values from the PGM configuration file that corresponds to the medium.

The VDS-IS software uses the following default TIBCOsmartPGM FX configuration files:

- fxd.conf.src
- fxd.conf.rcv

The SE stores sample versions of the default TIBCOsmartPGM FX configuration files in the /local/local1/multicast-expert-config/ directory for reference. You can modify one of these sample configuration files, and save it with the default filename. The modified configuration file becomes effective after the SE is restarted.

SEs contain the following sample configuration files:

- fxdSatellite.conf.src.sample—Use for a sender SE in a satellite network
- fxdSatellite.conf.rcv.sample—Use for a receiver SE in a satellite network
- fxdTerra.conf.src.sample—Use for a sender SE in a terrestrial network
- fxdTerra.conf.rcv.sample—Use for a receiver SE in a terrestrial network

To change the configuration parameters of a default TIBCOsmartPGM FX configuration file, follow these steps:

---

**Step 1** Log in to the multicast sender SE using FTP.

- a. From a PC running Windows, choose **Start > Run**.
- b. In the Open field, enter **ftp ipaddress**, using the IP address of the multicast sender or receiver SE.
- c. At the User prompt, enter your administrator-level username.
- d. At the password prompt, enter your password. The FTP prompt (ftp>) appears.

**Step 2** At the FTP prompt, open the multicast-expert-config directory:

```
ftp> cd multicast-expert-config
250 CWD command is successful.
ftp>
```

**Step 3** List the sample configuration files in the directory:

```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
fxdSatellite.conf.rcv.sample
```

```

fxdSatellite.conf.src.sample
fxdTerra.conf.rcv.sample
fxdTerra.conf.src.sample
226 Transfer complete.
ftp: 297 bytes received in 0.01Seconds 29.70Kbytes/sec.

```

Determine which sample file you want to retrieve, based on whether you are configuring the multicast sender or the receiver and whether your network is using terrestrial or satellite media transmission.

- Step 4** Return to binary mode from ASCII mode:

```

ftp> bin
200 Type set to I.

```

- Step 5** Copy the configuration file to your desktop:

```

ftp> get fxdSatellite.conf.rcv.sample
200 PORT command successful.
Opening BINARY mode data connection for fxdSatellite.conf.rcv.sample (5607 bytes).
226 Transfer complete.
ftp: 5607 bytes received in 0.00Seconds 5607000.00Kbytes/sec.
ftp>

```

- Step 6** End the FTP session:

```

ftp> quit

```

- Step 7** Locate the configuration file on your PC and open it using any text editor.

- Step 8** Edit the sample configuration file.

- Step 9** Save the file using **Save As**, and give it the same name as the default configuration file that you want to replace. For example, save the file named fxdSatellite.conf.rcv.sample as fxd.conf.rcv.

- Step 10** Transfer the file back to the multicast sender or receiver SE multicast-expert-config directory.

- Log in to the SE using FTP.
- Open the multicast-expert-config directory.
- Enter binary mode.
- Transfer the file into the directory. For example:

```

C:\>ftp 128.19.220.79
Connected to 128.19.220.79.
220 SERVICEENGINEING FTP server (Version wu-2.7.0(2) Tue Sep 7 17:20:20 P
DT 2004) ready.
User (128.19.220.79:(none)) :admin
331 Password required for admin.
Password:
230 User admin logged in. Access restrictions apply.
ftp> cd multicast-expert-config
250 CWD command successful.
ftp> bin
200 Type set to I.
ftp> put fxd.conf.rcv
200 PORT command successful.
150 Opening BINARY mode data connection for fxd.conf.src.
226 Transfer complete.
ftp:5607 bytes sent in 0.01Seconds 560.70Kbytes/sec.
ftp> quit

```

- Step 11** Restart the multicast sender or receiver SE for the new configuration to take effect.

## APIs for Multicast Cloud

The following APIs have been modified or added to support the configuration and monitoring of the Multicast Cloud feature:

- Multicast Cloud—MCastApiServlet API has been added with create, modify, and delete actions, as well as assign and unassign receiver SEs, and assign and unassign the Multicast Cloud to a Delivery Service
- Delivery Service—ChannelApiServlet API createDeliveryService and modifyDeliveryService actions have been modified with the ability to enable multicast for the Delivery Service
- Service Engine— CeApiServlet API seMulticast action has been added to enable an SE as a multicast sender and multicast receiver.

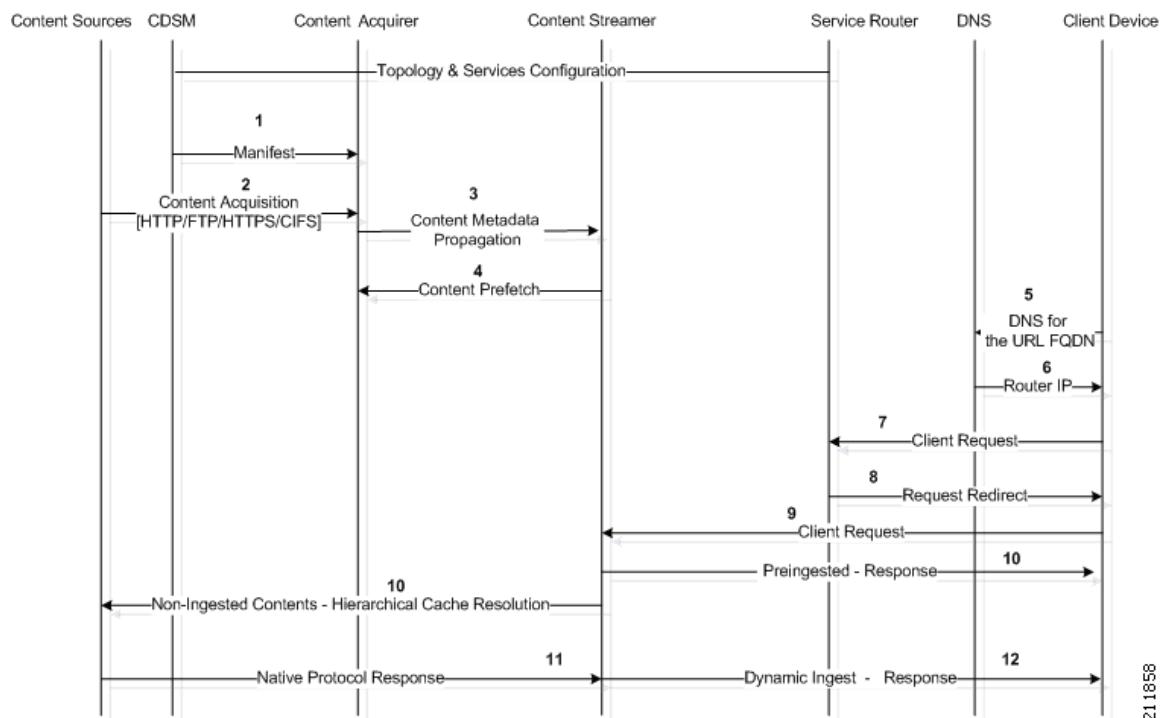
For more information, see the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 API Guide*.

## Service Workflow

What follows is a description of the workflow of a Delivery Service. [Table 2-1](#) shows sample values for the Delivery Service workflow described in [Figure 2-3](#). The Delivery Service workflow is described in detail following [Figure 2-3](#).

**Table 2-1      Delivery Service Parameters Example**

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

**Figure 2-3 Delivery Service Workflow Diagram**

1. The topology is propagated to all of the devices registered and activated in the Internet Streaming CDSM. The Delivery Service configuration is propagated to all of 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-internal.com/video/wmv-152>

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

## Programs

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.videonet.com/video/wmv-cached.wmv>

The Service Engines in the Delivery Service form a hierarchy, pull the content into the VDS-IS, 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.videonet.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.

# Programs

A program in the VDS-IS is defined as a scheduled live or rebroadcast event that streams content to client devices. The VDS-IS 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).

## 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 VDS-IS 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 Internet Streaming 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 Internet Streaming 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 Internet Streaming 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 Internet Streaming 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.

For more information, see Appendix A, “Program Files in the VDS-IS Software,” in the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 API Guide*.

## IPv6 Support for Client Interfaces

IPv6 is implemented on the client interfaces for the Web Engine, the Windows Media Streaming Engine, the Authorization Server, and the Service Router. Movie Streamer does not support IPv6.

**Note**

Starting with Release 3.3, Geo-Location Servers, DNS, Origin Servers, and NTP support both IPv6 and IPv4 addresses.

Communication among the VDS-IS Internet Streamer devices, between the VDS-IS and the Origin server, and with the CDSM GUI still uses IPv4; these communications includes CMS, Service Router keepalive, live routing, cache routing, and acquisition and distribution of content.

Because the VDS-IS supports dual stack (IPv4 and IPv6) for client interfaces, both IPv4 clients, IPv6 clients, and dual-stack clients can interact with the Internet Streamer.

The following rules apply to configuring IP addresses:

- For VDS-IS IPv6 support, manually configured IPv6 addresses are only used to communicate with the clients. Unique local IPv6 address and global IPv6 address can be configured for each interface.
- Unique local IPv6 address and global IPv6 address can be configured for each interface.
- Multiple IPv6 and IPv4 addresses can be assigned to each network interface.

An interface on a VDS-IS device (SE or SR) can learn auto-configured IPv6 addresses by way of stateless address autoconfiguration (SLAAC) from the default gateway interface.



**Note** When the default gateway interface IPv6 address is changed or removed, the associated interface on the VDS-IS device must be manually shut down and then brought back up, which is done by the **shutdown** command followed by the **no shutdown** command. This process removes the stale auto-configured IPv6 address and is required when the IPv6 addresses are changed or removed on the default gateway interfaces that connect to VDS-IS devices.

We recommend restarting the device if IPv6 is enabled or disabled as the safest method. Restarting (reloading) the device ensures that all of the processes are restarted and the kernel is functioning appropriately.



**Note** If the streaming interface configuration is changed (addition, deletion, modification), the Web Engine is restarted; therefore, we recommend offloading the SE before changing the streaming interface configuration.



**Note** The following are not supported for IPv6 addresses:

- IP Security (IPSec) implementation
- DHCP configuration
- Flash Media Streaming
- Movie Streamer
- Proximity-based routing
- Last-resort redirection

### Logical Interfaces

For the Service Engine, the logical interface configured as a primary interface must have an IPv4 address, because the intra VDS-IS device communication is only through IPv4. If the logical interface is configured as both a primary and a streaming interface, it must have both IPv4 and IPv6 addresses assigned, to serve IPv4 and IPv6, or dual stack clients.



**Note** Whenever the IP address of the primary interface is changed, the DNS server needs to be restarted.

For the Service Router, the primary interface must be configured with IPv4 and IPv6 address to serve IPv4 and IPv6 dual-stack clients.

### ICMP6, MLD, and Neighbor Discovery Messages

The following Internet Control Message Protocol version 6 (ICMPv6) messages are supported:

- ICMPv6 error messages
- Destination unreachable message
- Packet too big message
- Time exceeded message
- Parameter problem message

- Echo request message
- Echo reply message

The following Neighbor Discovery for IPv6 are supported:

- Router solicitation
- Router advertisement
- Neighbor solicitation
- Neighbor advertisement
- Redirect message

### DNS Configuration

The IPv6 address name server must be configured by using the **IPv6 name-server ip-address** command.



#### Note

The Service Router acts as the authoritative DNS server, and supports IPv6 DNS extensions.

If an IPv6 address is configured on the Service Router for DNS, the communication between the Service Router and the DNS server is over the IPv6 transport. The IPv4 address of the Service Router must be configured in the DNS server, so that the Service Router can respond to both A and AAAA queries. In this case, the communication between the DNS Server and the Service Router is over IPv4 transport.

### QoS

VDS-IS supports DSCP marking for QoS of outbound IPv4 or IPv6 traffic. The IPv4 header field is the Type of Service (ToS) or differentiated services code point (DCSP) value. The IPv6 header field is the Traffic Class (TCLASS).

### ACL Setting

Access control lists (ACLs) for IPv6 are separate from IPv4, and use the **Devices > Devices > General Settings > Network > IPv6 ACL** page. An ACL permit or deny policy for IPv6 traffic is based on source and destination IPv6 address, plus other IPv6 protocol factors, such as TCP, UDP, ICMPv6, and GRE, or a specific port number. There are two groups for IPv6 ACLs: Standard ACL and Extended ACL.

### Service Router

Communication between the Service Engine and Service Router is through the IPv4 stack, including the keepalive message. If IPv6 is enabled, then the keepalive message includes the IPv6 address of the SE in the keepalive message payload. This enables the Service Router to resolve the SE's IPv6 address correctly.

The Service Router operates as a DNS Server for the requests that belong to the Delivery Service to which the SR is associated. The Service Router is provisioned to respond to A or AAAA queries for the configured Service Routing Domain Name (RFQDN). The query can be on either an IPv4 or IPv6 transport.

The Service Router accepts the HTTP, RTSP, and RTMP requests and sends back the response by way of the IPv6 transport. The Service Router also supports the IP-based redirection, and includes the IPv6 address of the SE in the redirect URL. If the redirect URL has the SE host name, the client sends a DNS query to the Service Router, and the Service Router responds with the SE's IPv4 address for the A query and the SE's IPv6 address for the AAAA query.

The Coverage Zone file supports IPv6 and IPv4 addresses. The network and subnetwork addresses in the Coverage Zone file support CIDR format (IP address with a prefix).



**Note** Starting with Release 3.3, Geo-Location Servers, DNS, Origin Servers, and NTP support both IPv6 and IPv4 addresses.

---

### Authorization Server

The Authorization Server supports the following policies:

- IP address-based
- Geographic location-based
- Service rules-based

The Geo/IP file contains information on the allowed client IP addresses and geographic locations, and denied client IP addresses and geographic locations. The Authorization Server blocks client requests based on the Geo/Ip file uploaded for the Delivery Service. For IP address-based authorization, the Geo/Ip file supports both IPv4 and IPv6 addresses.

For geographic location-based authorization, the SE communicates with the Geo-Location server, which maps IP addresses to geographic locations. The Geo-Location server, which is the same Geo-Location sever used for location-based routing on the Service Router, identifies the geographic location of a client request by the country, state, and city of the client.



**Note** Starting with Release 3.3, Geo-Location Servers, DNS, Origin Servers, and NTP support both IPv6 and IPv4 addresses.

---

### Service Rules

For the Web Engine and Flash Media Streaming, Service Rules are configured by creating a Service Rule XML file and uploading it for the Delivery Service. The SrcIp pattern type supports both IPv4 and IPv6 addresses.

For Windows Media Streaming and Movie Streamer, Service Rules are configured on a per-device basis, either through the CDSM GUI or through the CLI. The **src-IPv6** pattern-list is used to configure IPv6 source patterns for Windows Media Streaming, and src-ip pattern-list is used to configure IPv4 source patterns for Windows Media Streaming and Movie Streamer.



**Note** Movie Streamer does not support IPv6 addresses.

---

### Windows Media Streaming Multicast

Windows Media Streaming multicast support provides a multicast service to distribute media efficiently to multiple clients using IP multicast. Before a client can tune into a channel and listen to or watch a stream, a multicast station has to be set up first. For IPv6 clients, the Windows Media Streaming multicast station should also multicast on an IPv6 multicast IP address. This requires that an IPv6 multicast IP address be configured for the live or rebroadcast program in the **Services > Live Video > Live Programs > Live Streaming** page for live programs and the **Services > Live Video > Live Programs > Streaming** page for rebroadcast programs.

The client fetches an NSC file to get the multicast IP address and port information. For IPv4 and IPv6 clients, Windows Media Streaming must generate two different NSC files. When Windows Media Streaming receives the request, the client type (IPv4 or IPv6) is detected and the corresponding NSC file is sent in the response.

# HTTPS Settings

The HTTPS Settings feature provides Delivery Service based HTTPS support for incoming requests to the SE and outgoing requests to the Origin server. The CDSM GUI offers the ability to enable HTTPS or HTTP for streaming to clients as well as ingesting from the Origin server for each Delivery Service. When the HTTPS feature is enabled, the inter-SE communication continues to use HTTP.

**Note**

HTTPS support for user equipment (UE) sessions is not supported by the Service Router, so the Service Router cannot be used to load-balance HTTPS sessions. DNS-based redirection must be used to redirect client requests.

DNS-based redirection means that service-aware routing and content-based routing cannot be used. For more information about DNS-based redirection, see the “[DNS-Based Redirection](#)” section on page 1-36.

---

The HTTPS feature supports SSL 3.0 and TLS 1.0 protocols to tunnel HTTP.

**Note**

Starting with Release 3.3, the HTTPS performance. The openssl library is upgraded to use crypto hardware acceleration. The performance for a CDE250 box with single unique cache-hit test is improved.

For the CDE machine only the CDE250 has AES-NI and the information to enable it in BIOS by hand or automatically by script.

For UCS bare metal and Virtual Machine (VM) has AES-NI support.

---

Starting with Release 3.3, the Generic Session Tracking and Logging supports HTTPS.

## Certificates

A certificate is installed if the SE is associated with a Delivery Service and the HTTPS settings is enabled.

Starting with Release 3.3, the SEs validate certificate of client. The client sends a certificate only when the Mutual Authentication is enabled. By default Mutual Authentication is disabled.

Also, starting with Release 3.3, the Certificate Revocation List (CRL) is supported. For more information about configuring the CRL certificates, see the “[Uploading a CRL File](#)” section on page 6-19.

Certificate Authority’s (CA’s) root certificates are expected to be available to all clients initiating HTTPS communication; most browsers are installed with well-known CA root certificates. Trusted CA certificates are expected to be provided for the purpose of Origin server certification validation.

VDS-IS does not support certificate enrollment (SCEP) nor certificate status verification (OCSP). The Internet service provider or third-party service provides enrolled certificates and installs them through the CDSM.

**Note**

---

A single subject alternative name (SAN) certificate is installed for all delivery services in the VDS-IS.

**HTTPS Settings****RSA Key Pair**

An RSA key pair (public, private) is generated and used for certificate signing requests (CSRs). The private key cannot be encrypted.

**Certificate and Key Pair Uploads to CDSM**

The **System > Configuration > HTTPS Settings** pages are used for uploading certificate files and key files.

**Updating Certificates**

When a new HTTPS Delivery Service is added or the Service Router domain name is changed on an existing HTTPS Delivery Service, the certificate and key file must be updated. This requires that new certificate and key files are uploaded to the CDSM and a schedule is created to notify the Web Engines associated with the affected HTTPS Delivery Service.



**Note** When the client sends a HTTPS connection to the Web Engine, and if the Service Router domain name is not matching the certificate's common name or ALT name, the connection will fail.

**Traffic Separation for HTTPS**

Prior to Release 3.0, port 443 was used for Acquisition and Distribution (A&D), all intra VDS-IS control, and management. With the introduction of the HTTPS feature, port 443 also needs to be used for streaming. It therefore becomes mandatory to have separate interfaces, one for the primary and one for streaming is mandatory. The management interface, if configured separately, must not share the same interface with the streaming interface.



**Note** The HTTPS feature supports the Multiple Logical IP addresses feature for multiple IP addresses for the streaming interface and one IP address for the primary interface. However, combining the streaming interface and the primary interface on one physical interface is not supported in the HTTPS feature.

**Primary Interface**

The primary interface is mandatory on all VDS-IS devices and consists of one or more physical interfaces, out of which one is always designated as the primary interface. The primary interface on the VDS-IS devices (SE, SR, and CDSM) is used for the following communication over port 443:

- Communication among SEs
- All intra VDS-IS control and data traffic
- All prefetched traffic from the Origin server to the SEs by way of the location tree
- All dynamic ingest and all cache miss traffic to the SEs by way of the location tree
- Finding routes to an Origin server for the cache router module and live stream module
- Keepalive information from the SEs to the SR
- All management communication between the SEs and the CDSM, by default

Alternatively, a management IP address and port can be configured manually on the SEs and SRs that are used for all management communication to the CDSM. For redundancy, a port channel can be configured. Streaming traffic uses the primary interface, and management traffic between the SE or SR and CDSM use the manually configured IP address and port, and if configured, the port channel and static route created for it.

**Note**

The Management Communication Port on the Device Activation page for an SE is hard-coded to port 443. The SR is not affected because the HTTPS feature does not support the SR. DNS-based redirection is the only routing redirection supported.

**Note**

To make sure that the SE or SR is binding to the primary interface (or management IP address, if configured) as the source IP address when sending management traffic to the CDSM, create a static route from the SE or SR to the CDSM. To configure a static IPv4 route from the SE or SR, see the “[Configuring Static Routes](#)” section on page 4-79. To configure a static IPv6 route from the SE or SR, see the “[Configuring Static IPv6 Routes](#)” section on page 4-80. Alternatively, you can use the **ip route** command and **IPv6 route** command on the VDS-IS device.

On higher-end CDEs, the primary interface can be configured as one-Gigabit Ethernet interface bonded as a port channel. The primary interface configuration is read-only from the CDSM, but it can be modified via the CLI to other interfaces.

**Note**

Whenever the IP address of the primary interface is changed, the DNS server needs to be restarted.

### Management IP and Port

After a primary interface has been selected, all CDSM-SE communication is via that interface. Optionally, a management IP address and port can also be specified for CDSM-SE communication and the primary interface would then be no longer be used. This interface can be disabled any time, in which case the primary interface is enabled for communication.

## Streaming Interface

After a primary interface has been configured and the device is online, the SE is ready to serve streaming traffic. By default, the traffic is served by the primary interface. Optionally, one or more streaming interfaces can be configured on an SE, which designates that all client-facing traffic goes through the streaming interface. Effective client throughput can be measured as a sum of traffic on all streaming interfaces.

The SE streaming interfaces have the following properties:

- If the HTTPS feature is not enabled, the streaming interface is optional, and can have the same IP address as the primary interface.
- The number of physical interfaces configured as streaming interfaces is not limited.
- They can be configured as a port channel.
- Multiple IP addresses in the same subnet can be configured for a streaming interface.
- The same IP address can be used for both a primary interface and a streaming interface.
- No intra CDN traffic goes through the streaming interface.
- Streaming interfaces can also be a single interface or a port channel.

The CDSM, SR, and other SEs do not know the IP addresses of the streaming interfaces on the SE; they only know the primary interface IP address. When the SE sends the SR keepalive messages, it sends the streaming interface IP addresses as well, which the SR uses to redirect requests to.

**HTTPS Settings****HTTPS Enabled**

To enable the HTTPS feature for a Delivery Service, the following configuration must exist:

- All SEs must have at least one streaming interface configured
- Streaming interface must be a different IP address than the primary interface (or management interface if configured)
- If a configured streaming interface needs to be reconfigured as a primary interface, the following command sequence must be followed to avoid a port 443 conflict and a failure to start the `rpc_httpd` process:

```
SE(config)# no streaming-interface GigabitEthernet 1/0
This box is configured to support HTTPS traffic delivery.
Deleting the only streaming interface configured will disable this functionality.
Do you want to continue? (Yes/No): yes
SE(config)# primary-interface GigabitEthernet 1/0
```



**Note** Before making configuration changes to the primary interface or management IP address on an SE, make sure that the CDSM is not performing updates to the SE, and there are no prefetching activities going on for the SE.



**Note** When the HTTPS feature is enabled, and configuration changes (addition, deletion, modification) are made to the streaming interfaces, the Web Engine is restarted; therefore, we recommend offloading the SE before changing the streaming interface configuration.

**Web Engine**

By default, the Web Engine uses port 80 of the primary interface on the SE for serving HTTP clients and communicating with the Origin server.

If a streaming interface is configured on the SE, the Web Engine uses port 80 of the streaming interface for serving HTTP clients and communicating with the Origin server.

If HTTPS is enabled on an SE, the Web Engine uses port 443 of the streaming interface for serving HTTPS clients.

Internally, the Web Engine on the SEs continue to use HTTP to communicate with each other.



**Note** If the HTTPS feature is disabled for a Delivery Service, the Web Engine on the SEs associated with that Delivery Service continue to use port 443.

**Configuring HTTPS**

Configuring the HTTPS feature consists of the following procedures:

- Uploading the Certificate and Key Files
- Separating the HTTPS Traffic
- Enabling HTTPS for a Delivery Service

**Uploading the Certificate and Key Files**

Uploading certificate and key files consists of the following pages:

- **Root CA File Registration**—Upload or import the certificates for the Origin servers participating in HTTPS
- **CRL File Registration**—Upload the Schedule the CRL for the Service Engine participating in HTTPS
- **CRL File Scheduling**—Schedule CRL file notification to the Web Engine on each SE that is participating in an HTTPS Delivery Service
- **HTTPS Certification Files Registration**—Upload client certificate and key file for all SEs
- **HTTPS Certification File Scheduling**—Schedule client certificate and key file notification to the Web Engine on each SE that is participating in an HTTPS Delivery Service

The procedures involved in uploading certificate and key files consist of the following:

- Uploading or Importing a Root CA File
- Uploading Client Certificate and Key Files
- Scheduling Web Engine Notification of Client Certificate and Key Files

For more information, see the “[HTTPS Settings](#)” section on page 6-17.

## Separating the HTTPS Traffic

To enable the HTTPS feature for a Delivery Service, all participating SEs must have at least one streaming interface configured and the streaming interface must be a different IP address than the primary interface (or management interface if configured).



### Note

Before making configuration changes to the primary interface or management IP address on an SE, make sure that the CDSM is not performing updates to the SE, and there are no prefetching activities going on for the SE.

When using the CLI to make configuration changes to the SE, it takes up to one data feed poll, which has a default of five minutes, for the CLI change to synchronize with the CDSM. Do not make any changes to the HTTPS setting, or SE assignment or device group assignment to the Delivery Service until the CDSM has been synchronized with the configuration change.



### Note

When the HTTPS feature is enabled, and configuration changes (addition, deletion, modification) are made to the streaming interfaces, the Web Engine is restarted automatically; therefore, we recommend offloading the SE before changing the streaming interface configuration.

To add a streaming interface to an SE, use the **streaming-interface** command. For more information, see the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference*. For more information about separating traffic, see the “[Traffic Separation for HTTPS](#)” section on page 2-26.

## Enabling HTTPS for a Delivery Service

To enable the HTTPS feature for a Delivery Service, all participating SEs must be configured with at least one streaming interface that has a different IP address than the primary interface (or management notifies if configured). For more information, see [Separating the HTTPS Traffic](#).

To enable HTTPS for a Delivery Service, see the “[Creating Delivery Service](#)” section on page 5-16.

## API Support for HTTPS

API support is provided for the HTTPS feature through the following APIs:

- ChannelApiServlet—Add the OsProtocol and StreamingProtocol parameters
- FileMgmtApiServlet—Add fileType setting of 26 for root certificate files
- CertKeyFileMgmtApiServlet—New Certificate Key File Management API



**Note** All parameters, except actions, are case sensitive.

If the action parameter is missing or cannot be recognized, an error code and the API usage syntax is returned.

For more information, see the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 API Guide*.

## Wholesale CDN

The Wholesale CDN feature offers the ability to configure delivery services with quotas and send real-time information to the Content Delivery Network Manager (CDNM) for managing wholesale (business-to-business) accounts.

The Wholesale CDN feature provides the following functions:

- [Session and Bandwidth Quotas per Delivery Service, page 2-30](#)
- [Cache Storage Priority per Delivery Service, page 2-32](#)
- [Snapshot Counters, page 2-32](#)
- [Real-Time Exporting of Transaction Logs for Billing and Analytic Reports, page 2-32](#)
- [APIs for Wholesale CDN, page 2-32](#)

## Session and Bandwidth Quotas per Delivery Service

Setting session and bandwidth quotas per Delivery Service in the VDS-IS, and associating a Delivery Service with a content provider (tenant) in the CDNM, provides the ability to manage multiple tenants with different session and bandwidth requirements in the CDNM.

The per-Delivery Service session quota limits the maximum number of concurrent sessions for that Delivery Service. The per-Delivery Service bandwidth quota limits the maximum bandwidth used to deliver content to clients.

The Service Router (SR) enforces the maximum limits (session quota and bandwidth quota) and tracks usage on each Service Engine (SE). The usage data is aggregated across the Delivery Service. The SR makes session enforcement decisions upon receiving requests to load balance. If the request for content does not exceed the maximum limit (quota threshold), it is routed to the best SE in the Delivery Service. If the request for content exceeds the maximum limit, the client receives an appropriate error response.



**Note** The session and bandwidth quotas do not reserve resources, nor do they guarantee service. The quotas only limit the maximum usage of a Delivery Service.

Release 3.1.0 only supports session and bandwidth quotas for Web Engine progressive download, Web

Engine adaptive bit rate (ABR), and Windows Media Streaming. Session and bandwidth quotas are not supported for Flash Media Streaming and Movie Streamer. The session and bandwidth quotas from Web Engine and Windows Media Streaming are aggregated in SR that makes the enforcement decision and the decision enforces all of the requests including Flash Media Streaming and Movie Streamer.

## Monitoring Session and Bandwidth Quotas

Information on quota allocation, usage, and denied sessions for each Delivery Service is sent to the CDNM. The CDN operator can monitor changes to the used quotas based on threshold crossing and session management metrics.

The SR transaction log has new status codes for session and bandwidth quotas being exceeded. The **show statistics service-router summary** command has new counters under “Requests Not Redirected” for “Session limit exceeded” and “Bandwidth limit exceeded.”

### Alarms and SNMP Traps

Each SE in the Delivery Service maintains a session counter and a bandwidth counter. The counters are sent to the SR over the keepalive messages.

The SR aggregates per-Delivery Service session and bandwidth counters and generates alarms and SNMP traps when session or bandwidth quotas are reached, and when augmented session or bandwidth quotas are reached. Clear alarms and corresponding SNMP traps are also sent when the quotas and augmented quotas return to normal. New incoming requests are still accepted if the quota threshold has been reached. New incoming requests are rejected if the augmented threshold has been reached. Both the quota thresholds and augmented quota thresholds are configurable per Delivery Service.

For both ABR and non-ABR sessions, the concurrent sessions counter is incremented when an end user request is received and a session is created on the SE, and decremented when the session is torn down. For ABR sessions, the concurrent sessions counter increments on receiving a manifest file request or a segment (fragment) request and decrements on finishing serving a manifest response or fragment response.

The following major alarms are generated by the SR if the quota thresholds are exceeded:

- DsSession—Session quota exceeded
- DsAugmentedSession—Augmented session quota exceeded
- DsBandwidth—Bandwidth quota exceeded
- DsAugmentedBandwidth—Augmented bandwidth quota exceeded

The quota threshold alarms include the Delivery Service ID that triggered the alarm. Whenever one of these alarms is raised or cleared the associated SNMP trap is sent (cdsAlarmMajorRaised and cdsAlarmMajorCleared respectively).

The following new OIDs have been added to the CISCO\_CDS\_SERVICE-ROUTING-MIB:

- cdssrRequestsSessionExceeded—Counter of the number of 499 events (not enough sessions)
- cdssrRequestsBandwidthExceeded—Counter of the number of 453 events (not enough bandwidth)

### Quota Reporting

Quota usage reporting is automatically sent whenever a session quota or a bandwidth quota is configured for a Delivery Service with a setting other than zero (zero means no limits are configured).

To monitor the session counter and bandwidth counter when session quota and bandwidth quota are not configured, check the **Force Quota Usage Reporting** check box in the General Settings page for the Delivery Service.

### Configuring Session and Bandwidth Quotas

Configure session and bandwidth quotas on the Definition page for the Delivery Service.

## Cache Storage Priority per Delivery Service

Assigning a cache storage priority to a Delivery Service enables the CDN operator with multiple tenants to provide preference settings for keeping cached content for a Delivery Service. By default, the Content Manager deletes cached content based on popularity (an algorithm involving the number of cache hits, the size of the content object, and the decay of the content object). The cache storage priority setting assigned to a Delivery Service influences the content popularity and thereby the content that is evicted.

To create cache storage priorities and assign them to Delivery Services, see the “[Creating Storage Priority Classes](#)” section on page 5-15.

## Snapshot Counters

The Snapshot Counter transaction logs for the SR and the SE record usage information per Delivery Service and can be sent to the CDNM for analytic reporting and billing purposes. For more information, see the “[Snapshot Counter Transaction Logs](#)” section on page 8-100.

## Real-Time Exporting of Transaction Logs for Billing and Analytic Reports

Transaction logs can be sent real-time from the SE and SR to the CDNM or other export server for use in analytic reports, summary billing records, and detailed transaction records on a per-Delivery Service basis. The SE and SR use the Splunk Universal Forwarder (UF) to push the transaction logs to the Splunk Lightweight Forwarder (LWF) on the CDNM.

For more information, see the “[Real-Time Exporting of Transaction Logs for Billing and Analytic Reports](#)” section on page 8-102.

## APIs for Wholesale CDN

The following APIs have been modified or added to support the configuration and monitoring of the Wholesale feature:

- Storage Priority Class—StoragePrioClassApiServlet API has been added with create, modify, and delete actions, and getStoragePrioClass action has been added to the ListApiServlet
- Quota Usage Reporting—New parameters have been added to the following actions of the ChannelApiServlet:
  - createDeliveryService
  - modifyDeliveryService
  - createDeliveryServiceGenSettings
  - modifyDeliveryServiceGenSettings

For more information, see the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 API Guide*.



## Getting Started

---

This chapter discusses initial device configuration, logging into and navigating the Internet Streaming Content Delivery System Manager (CDSM), and a typical Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS) configuration workflow.

- [Initially Configuring the Devices, page 3-1](#)
- [Logging In to the Internet Streaming CDSM, page 3-1](#)
- [Activating and Synchronizing the Devices, page 3-3](#)
- [Navigating the Internet Streaming CDSM, page 3-7](#)
- [Configuring Primary and Standby CDSMs, page 3-11](#)
- [Typical Configuration Workflow, page 3-13](#)

## Initially Configuring the Devices

You must initially configure the Content Delivery Engines (CDEs) before they can participate in the VDS-IS network. The CDE that runs the Internet Streaming CDSM must be initialized first so that the CDEs running the Service Engine (SE) and Service Router (SR) can register with it. For more information about initially configuring the CDEs, see the *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*.

After you have initially configured your CDEs, you must activate the SEs and SRs and configure the internal clocks by using the Internet Streaming CDSM. See the “[Activating and Synchronizing the Devices](#)” section on page 3-3 for more information.

## Logging In to the Internet Streaming CDSM

To log in to the Internet Streaming CDSM, follow these steps:

- 
- Step 1** Using your web browser, enter the IP address of your CDSM and port 8443.



**Note** VDS-IS supports Internet Explorer Version 6 or later, and Mozilla Firefox Version 3.6 or later.

For example, if the IP address of your CDSM is 192.168.0.236, enter:

**<https://192.168.0.236:8443>**

**Logging In to the Internet Streaming CDSM**

The Security Alert message is displayed.



**Note** If you are using Mozilla Firefox Version 3.6 or later as your web browser, you need to add the CDSM IP address to the exception list. After entering the CDSM IP address with port 8443, Firefox displays a Secure Connection Failed message with a link stating “Or you can add an exception.” Click this link, then click **Add Exception**. The Add Security Exception dialog box is displayed. Click **Get Certificate**, and then click **Confirm Security Exception**. The CDSM IP address is added to the exception list and you no longer receive the Secure Connection Failed message.



**Note** Sometimes the 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 CDSM, and enter the **no cms enable** command in global configuration mode followed by the **cms enable** command.

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

**Figure 3-1** *Internet Streaming CDSM Login Page*



- Step 3** Enter the username and password and click **Login**. The Internet Streaming CDSM home page is displayed.

The built-in username is *admin* and the initial password is *default*.



**Caution** You have only three attempts to login successfully. The CDSM will be locked, if you fail to login within three attempts.



**Note** The CDSM is locked for 30 minutes for a user, and is locked completely for an administrator.

**Note**

- It is strongly recommended that you change the built-in admin password as soon as possible. To do so, log in to the CLI of the CDSM device, and use the **username admin password <password>** global configuration command.
- If the default username and password have been changed by another CDSM administrator, you need to get the new username and password.

If you log in as an administrator, you can see the last login details along with the failed login details (if any).

Starting from release 4.0, VDS-IS allows the administrator user can view the list of locked user accounts, and unlock a user. via **System > AAA > Locked Users** page in the CDSM GUI. For more information to unlock a user, see “[Viewing Locked Users](#)” section on page 6-7.

## Activating and Synchronizing the Devices

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

**Caution**

All devices must be synchronized with each other for the VDS-IS to function properly.

Synchronization ensures accurate timestamps in all of 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 VDS-IS is the best practice.

**Note**

If the network is not configured with NTP, then every device in the VDS-IS 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 Internet Streaming CDSM, click one of the tabs (for example, Devices) and then one of the tab options (for example Locations).

**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), follow these steps:

**Step 1**

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

## Activating and Synchronizing the Devices

**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.



**Note** If the device that you want to activate is not listed in the Devices Table, restart the CMS for that device by telneting to it and entering the **no cms enable** command followed by the **cms enable** command in global configuration mode.

- 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**

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

Because the standby CDSM is global to the VDS-IS 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.

- b. 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 **Show All** above the Contents pane.

**Step 7** From the left-panel menu, choose **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 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 4-10](#)
- [Configuring NTP, page 4-64](#)

## Activating All Inactive Service Engines

To activate all inactive SEs, follow these steps:

**Step 1** From the 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**

Device Name	Type	IP Address	Status	Location	Software Version
NE-812-12	Service Engine	3.1.4.31	Online	NE-812-12-location	2.0.0.b.410
NE-812-5	Service Engine	3.1.4.14	Online	tier-1	2.0.0.b.400
NE-812-6	Service Engine	3.1.4.15	Online	tier-2	2.0.0.b.430

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

## Activating and Synchronizing the Devices

**Figure 3-5 Location Choice Page**



211811

- 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 of the inactive SEs shows “pending” until the devices have been fully activated.

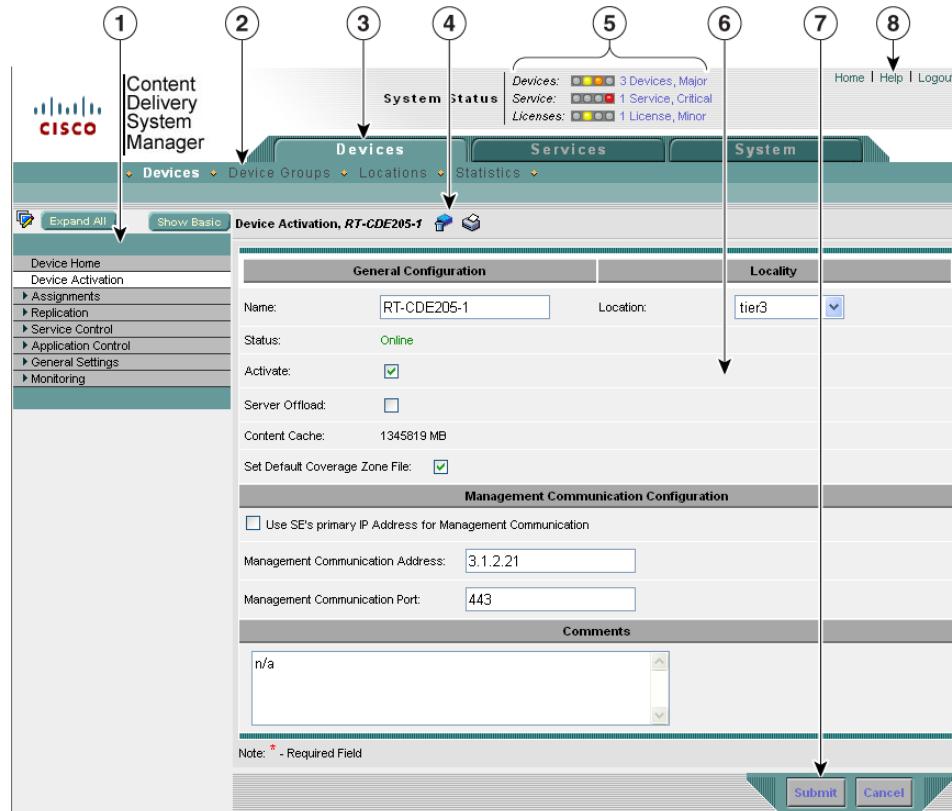


**Note** All devices activated in this way need to have the NTP settings configured. See [Step 6](#) through [Step 9](#) in the “Activating and Setting NTP for Each Device” section on page 3-3.

# Navigating the Internet Streaming CDSM

Figure 3-6 shows the different elements of the Internet Streaming CDSM.

**Figure 3-6 Internet Streaming CDSM User Interface**



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

The System Status bar, tabs, tab options, and tools are accessible from any page in the 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 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)

## Navigating the Internet Streaming CDSM

- Delivery Services (from Services tab)
- Live Video (from Services tab)

**Figure 3-7 Devices Table Page**

Devices						Services	System	
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			

<< Page 1 2 >> Showing 1-10 of 12 Devices 211803

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
- 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 VDS-IS 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 of 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 that you are on and provides associated tasks. All task bar icons, as well as other icons, have labels that are displayed when hover your mouse cursor over the icon.

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



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

**Table 3-1 CDSM Icons**

Icon	Function
A green icon showing a stack of three boxes with a small green switch-like symbol on the left.	Activates all inactive Service Engines.
A blue icon showing a stack of three boxes with a yellow pencil icon on the left.	Displays the devices.
A blue icon showing a stack of three boxes with a white square containing a blue arrow pointing right on the left.	Displays the left-panel menu.
A blue icon showing a stack of three boxes with a red circle containing a white minus sign on the left.	Deactivates the device.
A blue icon showing a stack of three boxes with a green arrow pointing right on the left.	Updates application statistics.
A blue icon showing a stack of three boxes with a red arrow pointing right on the left.	Forces the refresh of replication information or process content changes.
A blue icon showing a blue arrow pointing left on the left.	Goes back to the Replication Status page.
A blue icon showing a stack of three boxes with a blue circular arrow icon on the left.	Forces full database update.
A blue icon showing a stack of three boxes with a blue gear icon on the left.	Forces settings on SEs in the group.
A blue icon showing a stack of three boxes with a blue gear icon and a blue arrow pointing up-right on the left.	Forces the group settings.

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

Icon	Function
	Views read-only items.
	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 page.
	Copies a program.

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

Icon	Function
	Previews a program.
	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 CDSMs

The Internet Streaming CDSM can operate in two different roles: primary and standby. The primary role is the default. You can have only one primary CDSM active in your network; however, you can have any number of CDSMs operating in a standby role to provide redundancy and failover capacity. You must configure the primary CDSM first. See the *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide* for information on configuring the primary CDSM.



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

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

To configure a standby CDSM, follow these steps using the CLI:

---

**Step 1** Follow the instructions for configuring a CDSM using the setup utility, except do not enter the IP address of the CDSM. The instructions can be found in the *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*.

**Step 2** Configure the standby CDSM:

```
CDE(config)# cdsm role standby
```

**Step 3** Identify the IP address of the primary CDSM:

```
CDE(config)# cdsm ip 10.1.1.90
```

**Step 4** Start the Centralized Management System (CMS):

```
CDE(config)# cms enable
```

**Step 5** Save the configuration:

```
CDE# copy running-config startup-config
```

**Step 6** Activate the standby CDSM by using the web interface of the primary CDSM.

## Configuring Primary and Standby CDSMs

The primary CDSM notifies all registered devices that a standby 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 CDSM. Its function is to maintain an up-to-date copy of the primary's database.
- 

## Changing a Standby CDSM to a Primary CDSM



- Note** If your primary 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 CDSM operating at any given time.
- 

To change the standby CDSM to become the primary, follow these steps:

---

- Step 1** If your primary CDSM has failed, enter the following command:

```
CDE(config)# cdsm role primary
```

- Step 2** Save the configuration:

```
CDE# copy running-config startup-config
```

- Step 3** Restore the old primary CDSM, if possible:

- Step 4** When the old primary CDSM is restored, change its role to standby:

```
cdsm role standby
```

- Step 5** Reconnect the old primary CDSM (now the standby CDSM) into the VDS-IS network.

- Step 6** Wait at least one polling interval to allow the data from the primary CDSM to be copied to the standby CDSM.



- Note** During this period, do not make any configuration changes.
- 

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



- Note** There can only be one primary CDSM in a VDS-IS at one time. If there are two primary CDSMs, both CDSMs are halted.
- 

To do this, follow these steps:

- Change the role of the primary CDSM to standby:

```
cdsm role standby
```

- Change the role of the standby CDSM to primary:

```
cdsm role primary
```

**Note**

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

## Recovering from two Primary CDSMs

If you did not change the primary CDSM to standby before you changed the standby CDSM to primary, you will have two primary CDSMs in your VDS-IS and both will be halted. To restore both CDSMs, follow these steps:

- 
- Step 1** Make sure that the 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 CDSM by entering the **cms enable** command.
  - Step 3** Make sure the 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 CDSM by entering the **cms enable** command.
  - Step 5** Make sure that the standby CDSM is activated by using the web interface of the primary CDSM.
- 

## Typical Configuration Workflow

Once you have completed activating and configuring the NTP servers for all of the devices in the CDSM, you are ready to configure the VDS-IS 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 VDS-IS for content delivery, with references to the associated sections in each chapter.

## ■ Typical Configuration Workflow

**Table 3-2 Configuration Workflow**

Task	Description	Where to Find More Information
Change admin password	Change the administrator password on each device, including the CDSM, and change the administrator password for the system	<p>Log in to the CLI for the device and use the <b>username admin password &lt;password&gt;</b> global configuration command.</p> <p>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.</p> <p>To change the password for the CDSM GUI and CLI, go to “<a href="#">Creating, Editing, and Deleting Users</a>,” page 6-2</p>
Configure Dedicated Management with Redundant Port	Separate management traffic from application traffic, and configure a redundant port for management	<a href="#">“Configuring Port Channel,” page I-6</a>
Create Device Groups	Group like devices to speed up configuration	<a href="#">“Configuring Device Groups,” page 4-4</a>
Configure RCP	Configure Remote Copy Protocol (RCP) to listen for requests on TCP port 514	<a href="#">“Enabling RCP,” page 4-64</a>
Configure FTP	Enable FTP services to listen for connection requests	<a href="#">“Enabling FTP Services,” page 4-63</a>
Configure Web Engine	For all SEs participating in delivering content	<a href="#">“Configuring Web Engine HTTP Cache Freshness,” page 4-45</a>
Configure Windows Media Engine	For all SEs participating in delivering Windows Media content	Begins with <a href="#">“Configuring Windows Media Streaming—General Settings,” page 4-38</a>
Configure Movie Streamer	For all SEs participating in delivering MPEG or MOV content	<a href="#">“Configuring Movie Streamer—General Settings,” page 4-41</a>
Configure Flash Media Streaming	For all SEs participating in delivering Flash Media Streaming content	<a href="#">“Configuring Flash Media Streaming—General Settings,” page 4-43</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 VDS	<a href="#">“Coverage Zone File Registration,” page 6-12</a>
Configure Global Routing Method	Set the Coverage Zone file	<a href="#">“Configuring Global Routing,” page 6-14</a>
Configure Routing Method	Configure the routing method used by SRs	<a href="#">“Configuring the Service Router,” page 4-99</a>
Configure Content Origins	Define all origin servers that are used in delivery services	<a href="#">“Content Origins,” page 5-1</a>

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

Task	Description	Where to Find More Information
Create Delivery Service Definitions	Create delivery services for both prefetched or cached content and live programs	<a href="#">“Creating Delivery Service,” page 5-16</a>
Create Live Programs	Create live programs, or rebroadcasts and schedules	<a href="#">“Configuring Programs,” page 5-47</a>

**■ Typical Configuration Workflow**



# Configuring Devices

This chapter discusses configuring locations and device groups for devices, and detailed instructions on configuring the different types of devices—CDSMs, SEs, and SRs.

- [Configuring Locations, page 4-1](#)
- [Configuring Device Groups, page 4-4](#)
- [Configuring the Service Engine, page 4-9](#)
- [Configuring the Service Router, page 4-99](#)
- [Configuring the CDSM, page 4-131](#)

## Configuring Locations

Locations are set up in the Internet Streaming CDSM to organize and group SEs into virtual networks for distribution of content through delivery services. For more information about locations, see the “[VDS-IS Topology](#)” section on page 2-1.

Locations need to be configured before you can activate SEs and SRs and bring them online in the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS) network. [Table 4-1](#) describes the icons for the Locations Table page.

**Table 4-1 Location Icons**

Icon	Function
	Creates a new location.
	Creates a filtered table.
	Views all locations.
	Refreshes the table.

**Table 4-1 Location Icons (continued)**

Icon	Function
	Prints the current window.
	Edits a location.

To create a new location or edit an existing one, follow these steps:

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

**Figure 4-1 Locations Table Page**

The screenshot shows the Cisco Content Delivery System Manager interface. The top navigation bar includes 'Content Delivery System Manager', 'System Status' (Devices: 4 Devices, Critical; Service: 1 Service, Critical), and links for 'Home' and 'Logout'. Below the navigation is a menu bar with 'Devices', 'Services', and 'System' tabs, and dropdown menus for 'Devices', 'Device Groups', 'Locations', and 'Statistics'. The main content area is titled 'Locations' and contains a table with the following data:

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	

At the bottom of the table, there are buttons for '<< Page 1 >>' and 'Showing 1-7 of 7 Locations'. On the left side of the table, there is a 'Create New Location' button. The status bar at the bottom right shows '211801'.

- 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

The screenshot shows the 'Creating new Location' page within the Cisco Content Delivery System Manager. The top navigation bar includes links for Home and Logout. Below the navigation is a menu bar with tabs for Devices, Services, and System, and sub-options like Devices, Device Groups, Locations, and Statistics. The main content area is titled 'Creating new Location'. It contains a 'Location Information' section with fields for 'Name' (marked as required), 'ParentLocation' (set to 'None'), and 'Level' (set to '1'). Below this is a 'Comments' section with a text area. A note at the bottom states 'Note: \* - Required Field'. At the bottom right are 'Submit' and 'Cancel' buttons.

**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, in the Locations Table page, click the **Edit** icon next to the location that 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 that you configured when you assigned a parent to each location.

# Configuring Device Groups

The Internet Streaming 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 page.
	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 Service Engine” section on page 4-9.

To create or edit a device group, follow these steps:

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

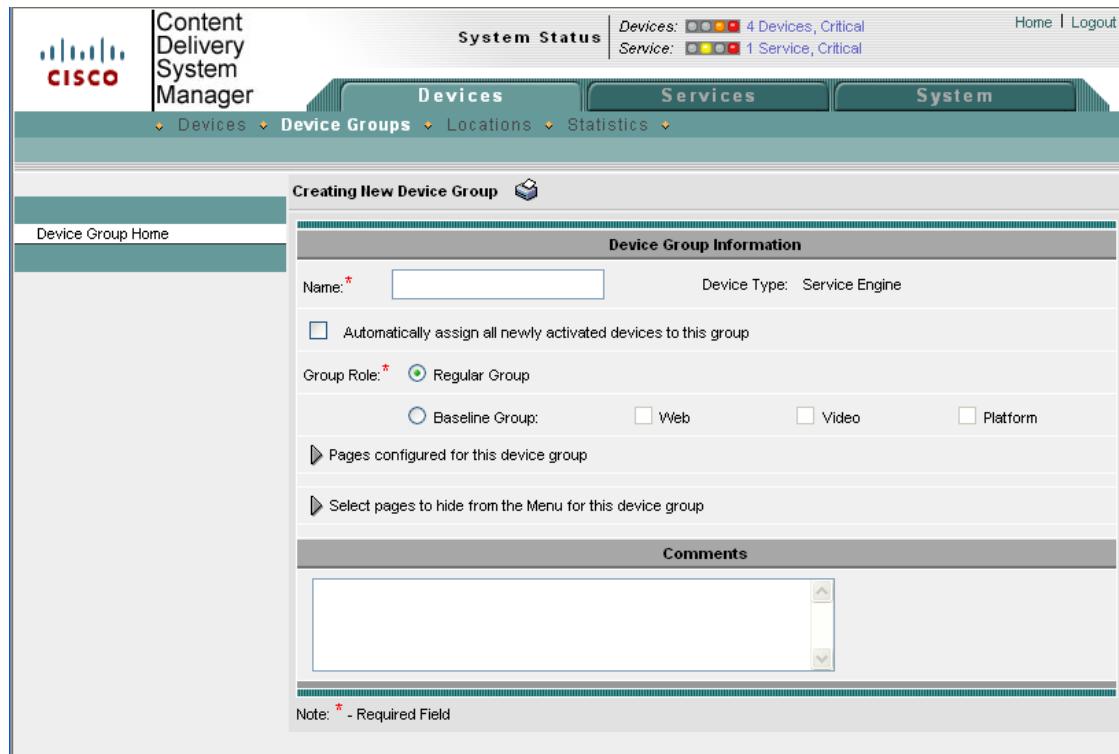
**Figure 4-3 Device Groups Table Page**



- 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 VDS-IS.
- Step 4** Check the **Automatically assign all newly activated devices to this group** check box if applicable.
- Step 5** Choose **Regular Group** to indicate that 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 that 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 VDS-IS.



**Note** From this point forward, the steps that you use to access a configuration page are combined into one step using menu options similar to the following: **Device Group > Assignments > Devices**.

**Step 10** Click the **Assign** icon (blue cross mark) next to each SE name that 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.

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

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



**Note** All SE settings in the “Configuring the Service Engine” 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 Windows Media Streaming—Bypass List” section on page 4-40 for more information.
- **Devices > General Settings > Network > Network Interfaces.** See the “Viewing Network Interfaces” section on page 4-68 for more information.
- **Devices > General Settings > Network > External IP.** See the “Configuring External IP Addresses” section on page 4-68 for more information.
- **Devices > General Settings > Network > IP ACL.** See the “Configuring IP ACL for IPv4 and IPv6” section on page 4-70 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 in the page and click **Submit**. The Device Group drop-down list displays “Select a Device Group.”

To reapply the settings for the device group, choose the device group from the Device Group drop-down list and click **Submit**. Alternatively, in the corresponding device group configuration page, click the **Force Settings on SEs in Group**. The **Force Settings on SEs in Group** only appears in 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.

**Note**

When adding an SE to an existing device group, the new SE does not automatically inherit the device group settings. Use the **Force Group Settings** option for the device group to force the group settings to all SEs in the group.

Alternatively, in each device group configuration page, click the **Force Settings on SEs in Group**. A dialog box appears listing all of the SEs that have different configuration settings than the device group settings. The **Force Settings on SEs in Group** only appears for a device group configuration page when an SE's individual settings override the group settings.

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 page.

## Aggregate Settings

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

- **Replication > Scheduled Bandwidth.** See the “Scheduled Bandwidth” section on page 4-18 for more information.
- **Service Control > Service Rules.** See the “Configuring Service Rules” section on page 4-21 for more information.
- **Service Control > URL Signing.** See the “Configuring URL Signing Key” section on page 4-27 for more information.
- **Application Control > Bandwidth Schedules.** See the “Configuring Bandwidth Schedules” section on page 4-36 for more information.
- **General Settings > Login Access Control > Users > Usernames.** See the “Creating, Editing, and Deleting Users—Usernames” section on page 4-55 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 that 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 that 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 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 corresponding device group 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 that the device uses.

Table 4-5 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.

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

Icon	Function
	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 page.

## 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, follow these steps:

- 
- 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 Service Engine

This section describes the different configuration pages available for a Service Engine. The main configuration groups are described as follows:

- **Replication**—Settings for bandwidth usage for replication and scheduling bandwidth usage. Additionally, distribution settings for negative acknowledgment (NACK) interval and multicast settings for designating an SE as a multicast receiver and sender.
- **Service Control**—Settings for access control by way of client request filtering, URL signing, and Authorization Server settings; additionally, transaction logs are configured to monitor traffic.
- **Application Control**—Settings for bandwidth management of delivery services and protocol engines (Web, Windows Media, Movie Streamer, Flash Media Streaming, and RTSP advanced settings).

- **General Settings**—Settings for access control of the device, maintenance, network connectivity, and monitoring.

The Device Activation page and the Assignments page, describes the activation of an SE in the Internet Streaming CDSM and assigning it to a location, and assigning device groups to the SE.

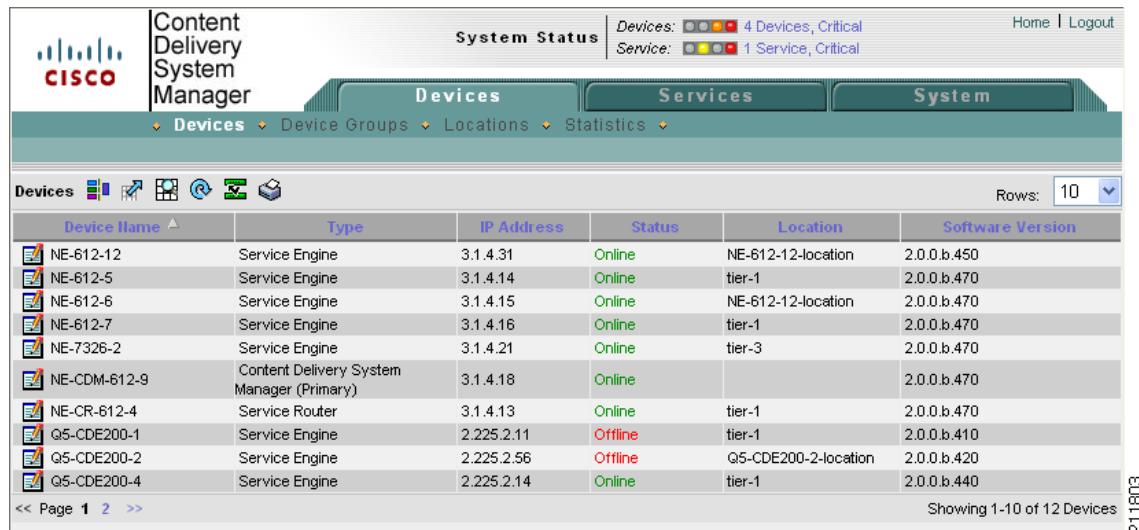
## Activating a Service Engine

Activating a device (Service Engine, Service Router, or standby 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, follow these steps:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed (Figure 4-5).

**Figure 4-5 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.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

Showing 1-10 of 12 Devices

211803

- Step 2** Click the **Edit** icon next to the device that 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 4-6).

**Figure 4-6 Device Activation Page**

**Step 4** Enter the settings as appropriate. See [Table 4-6](#) for a description of the fields.

**Table 4-6 Device Activation Fields**

Field	Description
Name	Name of the device.
Activate	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.  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 VDS-IS Network Device Registration Information</a> ” section on <a href="#">page 9-25</a> .

**Table 4-6 Device Activation Fields (continued)**

Field	Description
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, see the “<a href="#">Configuring Port Channel</a>” section on page I-6 for more information.</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 the Software</a>” section on page 9-6.</p> <p>The Status field in 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>
Content Cache	<p>Informational only. The content cache size is the total disk space on the VDS-IS 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 of 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>.</p>

**Table 4-6 Device Activation Fields (continued)**

Field	Description
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 a VDS-IS 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>,” page 6-12.</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 of the locations configured for the VDS-IS.
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 4-69 and the “<a href="#">Configuring Port Channel</a>” section on page I-6.</p>
Management Communication Port	Port number to enable communication between the CDSM and the SE.
Billing Cookie	<p>Enables the administrator to enter the Billing Cookie string used in customer billing transactions occurring in a given streamer. The range is from 1 to 256 characters and the default value is “-”. Space is not allowed in Billing Cookie string. CDSM reports error if these conditions are violated.</p> <p><b>Note</b> This field is logged in all web-engine &amp; acquisition and distribution transaction logs.</p>
Comments	Information about the settings.

**Note**

To make sure that the SE is binding to the primary interface (or management IP address if configured) as the source IP address when sending management traffic to the CDSM, create a static route from the SE to the CDSM. To configure a static IPv4 route from the SE, see the “Configuring Static Routes” section on page 4-79. To configure a static IPv6 route from the SE, see the “Configuring Static IPv6 Routes” section on page 4-80. Alternatively, you can use the **ip route** command and **IPv6 route** command on the VDS-IS device.

- 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, follow these steps:

- Step 1** Choose **Devices > Devices**, and click the **Edit** icon next to the device that 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 4-7).

**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 4-7 Assignment Page**

Device Group assignments for Service Engine, NE-612-12		
Device Group	Device Type	Comments
NorthBay	Service Engine	
SouthBay	Service Engine	

- Step 3** Click the **Assign** icon (blue cross mark) next to the device group that 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 that indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon. The SE assignment states are described in [Figure 4-8](#).

**Figure 4-8 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.

---

## Replication

The bandwidth used for replication and ingest is determined by the settings in the Default Bandwidth and the Scheduled Bandwidth pages. The replication configuration pages consist of the following:

- [Default Bandwidth, page 4-16](#)
- [Scheduled Bandwidth, page 4-18](#)
- [Configuring the NACK Interval Multiplier, page 4-20](#)
- [Enabling SEs for Multicasting, page 4-20](#)

[Table 4-7](#) describes the icons on the replication bandwidth configuration pages.

**Table 4-7 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.

**Table 4-7 Replication Bandwidth Configuration Icons**

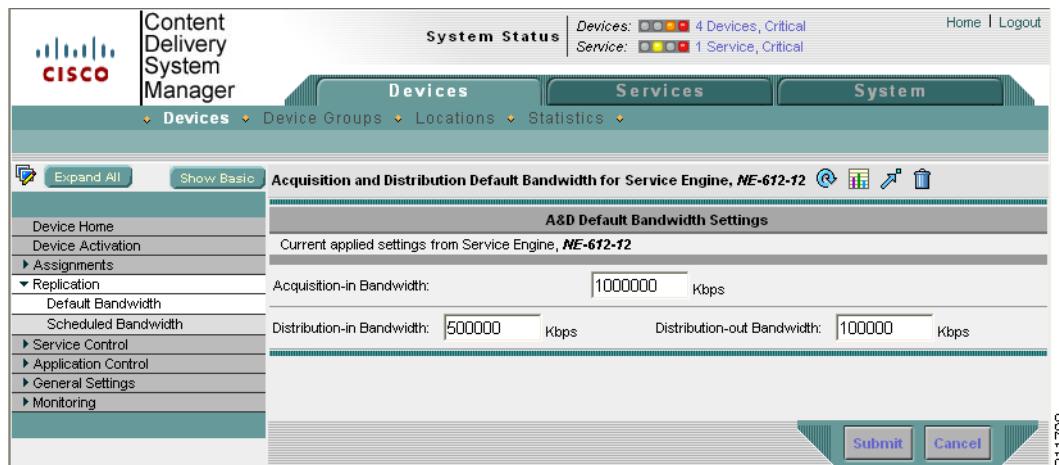
Icon	Function
	Prints the current page.
	Edits a scheduled bandwidth. Click this icon next to one of the scheduled bandwidths to edit the settings.
	Deletes a scheduled bandwidth. To delete a scheduled bandwidth, click the <b>Edit</b> icon and then click this icon.

## 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, follow these steps:

- Step 1** Choose **Devices > Devices > Replication > Default Bandwidth**. The Replication Default Bandwidth page is displayed (Figure 4-9).

**Figure 4-9 Replication Default Bandwidth Page**

- Step 2** Enter the settings as appropriate. See Table 4-8 for a description of the fields.

**Table 4-8 Replication Default Bandwidth Fields**

Field	Description
Acquisition-in Bandwidth	Bandwidth used for ingesting content when this SE is acting as the Content Acquirer. The default is 1,000,000 kbps (kilobits per second).

**Table 4-8 Replication Default Bandwidth Fields**

Field	Description
Distribution-in Bandwidth	Bandwidth used for incoming content that is sent by a forwarding SE as part of the distribution process. The default is 500,000 kbps.
Distribution-out Bandwidth	Bandwidth used for outgoing content that is sent to a downstream SE as part of the distribution process. The default is 100,000 kbps.

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

For information on the task bar icons, see [Table 4-7](#).

### 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 page.

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 4-9](#).

**Table 4-9 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	Toggles between the two options:  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.  Show Effective Bandwidth—Displays the composite (aggregate) bandwidth settings for the SE and its associated device groups.

**Table 4-9 Acquisition and Distribution Bandwidth Graph—Viewing Options (continued)**

Option	Description
Show Aggregate View/Show Non-Aggregate View	Toggles between the two options: Show Aggregate View—Displays the bandwidth settings configured for the corresponding device groups. Show Non-Aggregate View—Displays the bandwidth settings configured for the SE.
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.

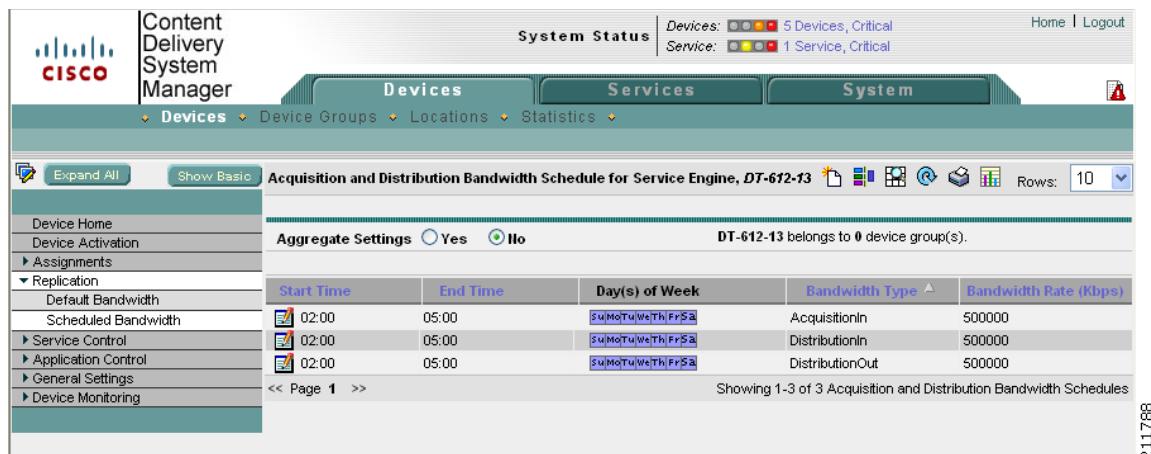
## Scheduled Bandwidth

Scheduled Bandwidth settings take precedence over Default Bandwidth settings.

To configure a bandwidth schedule, follow these steps:

- 
- Step 1** Choose **Devices > Devices > Replication > Scheduled Bandwidth**. The Replication Scheduled Bandwidth Table page is displayed (Figure 4-10).

The table is sortable by clicking the column headings.

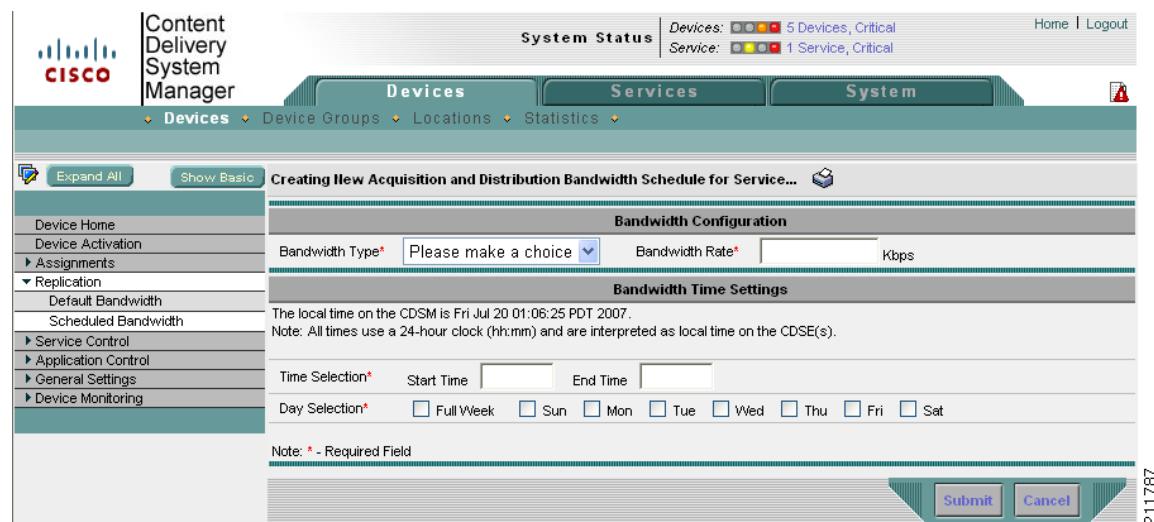
**Figure 4-10 Replication Scheduled Bandwidth Table Page**

For information about Aggregate Settings, see the “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 4-11).  
To edit a scheduled bandwidth, click the **Edit** icon next to the scheduled bandwidth that you want to edit.

**Figure 4-11 Replication Scheduled Bandwidth Page**

**Step 3** Enter the settings as appropriate. See [Table 4-10](#) for a description of the fields.

**Table 4-10 Replication Scheduled Bandwidth Fields**

Field	Description
Bandwidth Type	<p>Distribution-in—For incoming content distribution traffic from SEs.</p> <p>Distribution-out—For outgoing content distribution traffic to SEs.</p> <p>Acquisition-in—For incoming content acquisition traffic from origin servers.</p> <p><b>Note</b> The maximum bandwidth for Distribution-in, Distribution-out, and Acquisition-in bandwidth is 1 Gbps.</p> <p>Multicast-out—For outgoing multicast content traffic to SEs.</p> <p><b>Note</b> The Multicast Cloud feature is for early field trials (EFTs) and is not supported in Release 3.1.0.</p>
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	<p>Days on which bandwidth settings apply.</p> <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 4** Click **Submit** to save the settings.

For information on the task bar icons, see [Table 4-7](#).

## Configuring the NACK Interval Multiplier

To identify missing content and trigger a resend of a file, the receiver SEs send a negative acknowledgment (NACK) message to the sender SE. NACK messages generated by many receiver SEs could generate more traffic than the sender can handle. The NACK interval multiplier allows you to adjust the average interval between NACKs for an individual receiver SE. This value (a percentage from 10 to 100 percent of normal, to a multiple of normal from 2 times to 10 times) adjusts the default average NACK interval. The default or normal setting is 20 minutes. As an example, if the NACK interval multiplier is set to 3, the interval between NACKs becomes 20 minutes x 3, or 60 minutes.



**Note** The Multicast Cloud feature is supported in all releases starting with Release 3.1.1.

To send an immediate NACK request rather than wait for the scheduled interval, enter the **distribution multicast send-nack-now** command on a multicast receiver SE.

To configure the NACK interval multiplier, follow these steps:

- 
- Step 1** In the CDSM GUI, choose **Devices > Devices > Replication > Distribution**. The Distribution page is displayed.
  - Step 2** Click and drag the **Content NACK Interval Multiplier** slider control across the calibrated ruler to adjust the interval between NACK messages. The scale ranges from 10 percent of normal to 10 times normal. The center of the scale corresponding to “normal” denotes the default of 20 minutes. The value corresponding to the slider position is displayed to the right of the slider.
  - Step 3** Click **Submit** to save the settings.
- 

## Enabling SEs for Multicasting

Before you can create a Multicast Cloud, the SEs must be enabled for multicasting. These multicast-enabled SEs can then be assigned as sender and receiver SEs of a Multicast Cloud.



**Note** The Multicast Cloud feature is supported in all releases starting with Release 3.1.1.

To enable SEs for multicasting, follow these steps:

- 
- Step 1** From the CDSM GUI, choose **Devices > Devices > Replication > Multicast Distribution**. The Multicast Distribution page is displayed.
  - Step 2** Check the **Enable multicast receiver** check box if this SE is to act as a multicast receiver.  
Check the **Enable multicast sender** check box if this SE is to act as a multicast sender.
  - Step 3** Click **Submit** to save the settings.
-

## Service Control

The Service Control pages provide settings for client request filtering, URL signing, and Authorization Server settings. Additionally, transaction logs that monitor traffic are configured under the Service Control. Configuring service control consists of the following procedures:

- [Configuring Service Rules, page 4-21](#)
- [Configuring URL Signing Key, page 4-27](#)
- [Configuring the Authorization Service, page 4-28](#)
- [Configuring Transaction Logs, page 4-30](#)

[Table 4-11](#) describes the icons for the Service Control pages.

**Table 4-11 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 page.
	Edits an item.
	Deletes an item. To delete an item, click the <b>Edit</b> icon and then click this icon.

## Configuring Service Rules



**Note** This is a licensed feature. Please ensure that you have purchased a Service Rule license for this advanced feature.

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 data feed poll rate, then the device goes offline until the processing is completed. You can avoid this by configuring a higher data feed poll rate. The recommended data feed poll rate for 750 Service Rules is 300 seconds. To configure the data feed poll rate, see the “[Configuring System Settings](#)” section on page 6-8.

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.

To configure or edit Service Rule settings, follow these steps:

---

**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.

**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.

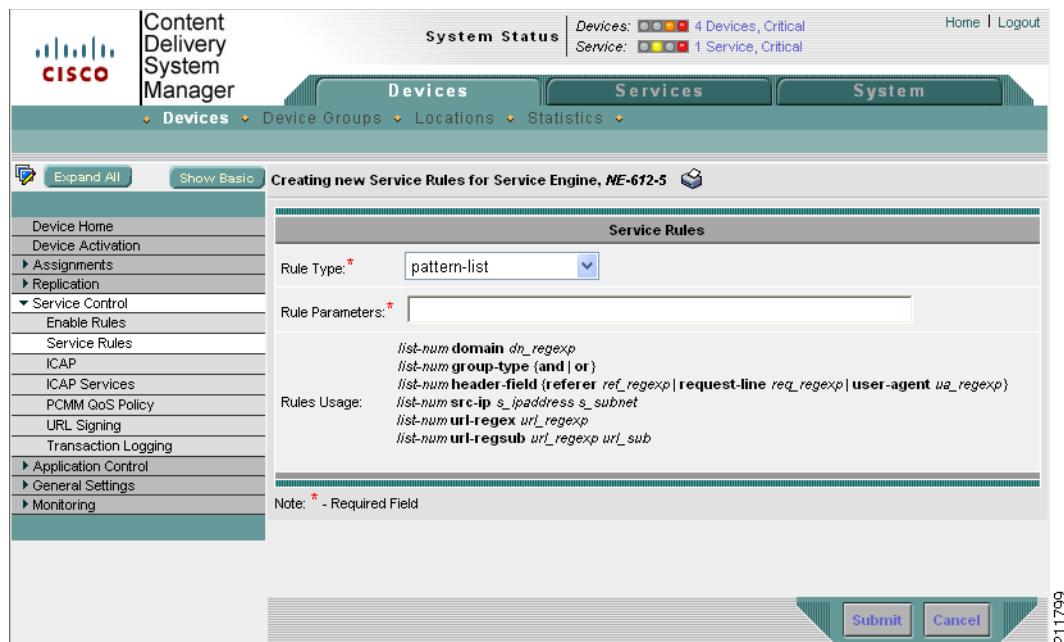
The table is sortable by clicking the column headings.

For information about Aggregate Settings, see the “[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 4-12).

To edit a Service Rule, click the **Edit** icon next to the Service Rule that you want to edit.

Figure 4-12 Service Rules Page



211799

**Step 6** 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 in the Service Rule page. See [Table 4-12](#) 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 example.com domain as the domain to be acted on, enter **72 domain example.com** in the **Rule Parameters** field.

**Table 4-12** Service Rules Pattern Types

Pattern Type	Description	Syntax
domain	<p>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.</p> <p>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.</p>	<b>rule pattern-list list_num</b> <b>domain dn_regexp</b>
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 list-num</b> <b>group-type {and   or}</b>

**Table 4-12** 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> <b>header-field</b> { <b>referer</b> <i>ref_regex</i>   <b>request-line</b> <i>req_regex</i>   <b>user-agent</b> <i>ua_regex</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> <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> <b>url-regex</b> <i>url_regex</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> <p><b>Note</b> Only one url-regsub pattern list is supported. Multiple substitutions for the same pattern list are not supported.</p>	<b>rule pattern-list</b> <i>list_num</i> <b>url-regsub</b> <i>url_regex url_sub</i>



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 4-99 for more information about IP-based redirection. Flash Media Streaming bypasses the rules configuration if the request is from another SE.

**Step 7** Click **Submit** to save the settings.

The maximum number of pattern lists allowed is 128.

**Step 8** Associate an action with an existing pattern list.

- Choose an action type from the Rule Type drop-down list. See [Table 4-13](#) for a description of rule actions.
- 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 example.com, then choose **block** from the Rule Type drop-down list, and enter **pattern-list 72 protocol all** in the Rule Parameters field.

**Note**

For the Web Engine and Flash Media Streaming, the Service Rule file must be used if Service Rules are to be configured.

**Note**

All Windows Media Streaming per-device Service Rules configured for URL signature and validation must be converted to the per-Delivery Service Rule XML file. This change only applies to the generate-url-signature and validate-url-signature Service Rule actions for Windows Media Streaming. The other Service Rule actions (allow, block, no-cache, redirect, refresh, replace, and rewrite) still use the per-device Service Rule configuration for Windows Media Streaming. For more information, see the “[Converting Old Windows Media Streaming Service Rules for URL Signing and Validation](#)” section on page E-25.

**Note**

Windows Media Streaming supports all Service Rule actions listed in [Table 4-13](#), except validate-url-signature. Movie Streamer supports the following Service Rule actions: allow, block, redirect, rewrite, and validate-url-signature.

**Table 4-13** **Service Rule Actions**

Action Type	Description	Syntax
allow	Allows incoming requests that match the pattern list. 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> <i>list_num [protocol {all   http   rtmp   rtsp}]</i>
block	Blocks this request and allows all others.	<b>rule action block pattern-list</b> <i>list_num [protocol {all   http   rtmp   rtsp}]</i>
no-cache	Does not cache this object.	<b>rule action no-cache pattern-list</b> <i>list_num [protocol {all   http   rtmp   rtsp}]</i>
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 <i>url</i> pattern-list</b> <i>list_num [protocol {all   http   rtmp   rtsp}]</i>
refresh	For a cache hit, forces an object freshness check with the server.	<b>rule action refresh pattern-list</b> <i>list_num [protocol {all   http}]</i>
replace	Replace the text string in the object.	<b>rule action replace <i>string_to_find</i> <i>string_to_replace</i> pattern-list</b> <i>list_num [protocol {all   http   rtmp   rtsp}]</i>

**Table 4-13** Service Rule Actions (continued)

Action Type	Description	Syntax
rewrite	Rewrites the original request as a specified URL.	<b>rule action rewrite pattern-list</b> <i>list_num</i> [ <b>protocol</b> {all   http   rtmp   rtsp}]
validate-url-signature	<p>Validates the URL signature for a request using the configuration on your SE for the URL signature and allows the request processing to proceed for this request.</p> <p>The <b>error-redirect-url</b> keyword redirects requests that failed validation to a specified URL. The <b>error-redirect-url</b> keyword is only supported for HTTP URLs.</p> <p>The <b>exclude</b> keyword excludes the client IP address, the content expiry time, domain, or both the client IP address and expiry time from the URL signature validation, and redirects requests that failed validation to a specified URL.</p> <p>The <b>exclude client-ip</b> keywords instruct the SE to ignore the client's IP address when processing the validation of the signed URL. The command could be configured as <b>rule action validate-url-signature exclude client-ip error-redirect-url aa pattern-list 1 protocol all</b>.</p> <p>The <b>exclude expiry-time</b> keywords instruct the SE to ignore the expiry time that normally limits access to the content when the expiry time has occurred. The command could be configured as <b>rule action validate-url-signature exclude expiry-time error-redirect-url pattern-list 1 protocol all</b>.</p> <p>The <b>exclude domain-name</b> keyword instructs the SEs to ignore the domain in the URL when processing the validation of the signed URL. The command could be configured as <b>rule action validate-url-signature exclude domain-name error-redirect-url pattern-list 1 protocol all</b>.</p> <p>The <b>exclude all</b> keywords instruct the SE to ignore both the client IP address and the content expiration time when processing the validation of the signed URL. The command could be configured as <b>rule action validate-url-signature exclude all error-redirect-url aa pattern-list 1 protocol all</b>.</p>	<b>rule action validate-url-signature</b> { <b>error-redirect-url</b> <i>url</i>   <b>exclude</b> { <b>all</b>   <b>error-redirect-url</b> <i>url</i>   <b>client-ip</b>   <b>error-redirect-url</b> <i>url</i>   <b>expiry-time</b>   <b>error-redirect-url</b> <i>url</i>   <b>domain-name</b> <b>error-redirect-url</b> <i>url</i> }   <b>pattern-list</b> <i>list_num</i> [ <b>protocol</b> { <b>all</b>   <b>http</b>   <b>rtmp</b>   <b>rtsp</b> }]}

**Step 9** Click **Submit** to save the settings.



**Note** When configuring Service Rules, you must configure the same Service Rules on all SEs participating in a Delivery Service 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.

## Execution Order of Rule Actions

The order in which the rule actions are implemented for Windows Media Streaming and Movie Streamer 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 of 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 implementation 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)

**Note**

For the Web Engine and Flash Media Streaming, the Service Rule file must be used if Service Rules are to be configured. See the [Appendix E, “Creating Service Rule Files.”](#) for more information.

## Configuring URL Signing Key

URL signature keys are word values that ensure URL-level security. The URL signature key is a shared secret between the device that assigns the key and the device that decrypts the key. Based on your network settings, either the SE itself or some other external device can assign the signature key to the URL, but the SE decrypts the URL signature key.

The VDS-IS uses a combination of key owners, key ID numbers, and a word value to generate URL signature keys. You can have a maximum of 32 key owners. Each key owner can have up to 16 key ID numbers.

To create request-specific URL signature keys, you can choose to append the IP address of the client that has made the request to the URL signature key.

To create a URL signature key, follow these steps:

---

**Step 1** Choose **Devices > Devices > Service Control > URL Signing**. The URL Signing Table page is displayed.

The table is sortable by clicking the column headings.

For information about Aggregate Settings, see the [“Aggregate Settings” section on page 4-8](#).

**Step 2** Click the **Create New** icon in the task bar. The URL Signing page is displayed.

To edit the URL signature, click the **Edit** icon next to the URL Signature Key ID owner that you want to edit.

**Step 3** Enter the settings as appropriate. See [Table 4-14](#) for a description of the fields.

**Table 4-14 URL Signature Key Settings**

Field	Description
Cryptographic Algorithm	Choose either <b>Symmetric Key</b> or <b>Asymmetric Key</b> . For more information, see the “URL Signing and Validating” section on page H-6.
Key ID Owner	Specify the ID number for the owner of this encryption key. Valid entries are from 1 to 32.
Key ID Number	Specify the encryption key ID number. Valid entries are from 1 to 16.
Key	Field for <b>Symmetric Key</b> only. Enter a unique URL signature key with up to 16 characters (excluding double quotes at the beginning and end of the string). This field accepts only 7-bit printable ASCII characters (alphabetic, numerics, and others) and does not support a space or the following special characters: pipe ( ), question mark (?), double quotes ("), and apostrophe ('). The following special characters are allowed: {}!#\$%&()*+,-./;:<=>@\~^[]_ Quoted and unquoted strings are allowed. Double quotes ("") are allowed at the beginning and end of the string only. If you do not surround the key string with double quotes, quotes are added when you click <b>Submit</b> .
Public Key URL	Field for <b>Asymmetric Key</b> only. The location of the public key file. Only HTTP, HTTPS, or FTP addresses are supported. The public/private key pair is stored in Privacy Enhanced Mail (PEM) format. <b>Note</b> While Validation, the public key file is checked if the file size exceeds 2000 bytes and if the file starts with "-----BEGIN PUBLIC KEY-----" and contains "-----END PUBLIC KEY-----" line
Private Key URL	Field for <b>Asymmetric Key</b> only. The location of the private key file. Only HTTP, HTTPS, or FTP addresses are supported. The public/private key pair is stored in Privacy Enhanced Mail (PEM) format. <b>Note</b> While Validation, the private key file is checked if the file size exceeds 2000 bytes and if the file starts with "-----BEGIN EC PRIVATE KEY-----" and contains "-----END EC PRIVATE KEY-----" line
Symmetric Key	Field for <b>Asymmetric Key</b> only. A 16-byte American Encryption Standard (AES) key used for AES encryption of the signed URL.

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

For information on the URL signing mechanism, see [Appendix H, “URL Signing and Validation.”](#)

## 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 or geographic location 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 service routing fully qualified domain name (RFQDN) or origin server FQDN (OFQDN) that is recognized as part of a Delivery Service. For more information about RFQDNs and origin server, see the “Content Origins” section on page 5-1. If you want to allow client requests for unknown hosts, check the **Enable Unknown-Server Requests** check box.

**Note**

The string “.se.” cannot be used in the RFQDN and OFQDN.

To block client requests based on geographical location, the SE communicates with a Geo-Location server, which maps IP addresses to a geographic locations. The Geo-Location server, which is the same Geo-Location server used for location-based routing on the SR, identifies the geographic location of a client request by the country, state, cit, netspeed, connection type, linespeed, asn, and carrier of the client. See the “[Configuring Request Routing Settings](#)” section on page 4-104. For more information about the Geo-Location servers, see the “[Geo-Location Servers](#)” section on page 4-107.

Each Delivery Service participating in the Authorization Service has a Geo/IP 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 Geo/IP 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 “[Authorization Plugins](#)” section on page 5-27

To enable the Authorization Service, follow these steps:

**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.

The Authorization Service is enabled by default.

**Step 3** To disable the Geo Plugin on this SE, uncheck the **Enable Geo Plugin** check box. The Geo Plugin is enabled by default.

The Geo/Ip Plugin is configured for each Delivery Service that has a Geo/Ip file associated. Every SE in the Delivery Service contacts the Geo-Location server to look up the client IP address for the allowed geographical locations. However, not every SE needs to contact the Geo-Location server (for example, upstream SEs). Disabling the Geo Plugin on upstream SEs reduces the number of times the Geo-Location server is contacted.

**Step 4** In the **Cache Timeout** field, enter the timeout interval (in seconds) that a response from the Geo-Location server is stored in the SE cache. The SE caches information from the Geo-Location server during the first request so that further requests can be served from cache instead of contacting the Geo-Location server.

The default is 691200. The range is 1 to 864000.

**Step 5** From the **Type** drop-down list, choose one of the following server types:

- Quova—if **quova** is selected from the **Type** drop-down list:
  - In the **Primary Address** and associated **Port** fields, enter the IPv4 address and port number of the primary Geo-Location Server.
  - In the **Secondary Address** and associated **Port** fields, enter the IPv4 address and port number of the secondary Geo-Location Server.
- Quova GDS (Version 7.1.5)—If **quova-restful-gds** is selected form the Type drop-down list:
  - In the **Primary Address** and associated **Port**, **Service Name**, **Retry** and **Timeout** fields, enter the IPv6 or IPv4 address, port number, Service name, Retry, and Timeout of the primary Geo-Location Server.

- In the **Secondary Address** and associated **Port**, **Service Name**, **Retry** and **Timeout** fields, enter the IPv6 or IPv4 address, port number, Service Name, Retry, and Timeout of the secondary Geo-Location Server.
- Quova Hosted—if **quova-restful-hosted** is selected from the **Type** drop-down list:
  - In the **API Key** field, enter the API key of the Geo-Location Server.
  - In the **Shared Secret Key** field, enter the shared secret key of the Geo-Location Server.
  - In the **Primary Address** and associated **Port**, **Service Name**, **Retry** and **Timeout** fields, enter the IPv6 or IPv4 address, port number, Service Name, Retry, and Timeout of the primary Geo-Location Server.
  - In the **Secondary Address** and associated **Port**, **Service Name**, **Retry** and **Timeout** fields, enter the IPv6 or IPv4 address, port number, Service Name, Retry, and Timeout of the secondary Geo-Location Server.
- MaxMind Hosted—if the **maxmind-restful-hosted** is selected from the **Type** drop-down list:
  - From the **Protocol** drop-down list, choose **Http** or **Https**.
  - In the **Service** field, enter the service name. The service name can be a, b, f, or e.
  - In the **License Key** field, enter the key that is used by the Geo-Location server to verify a request.
  - In the **Primary Address** and associated **Port**, **Retry** and **Timeout** fields, enter the IPv6 or IPv4 address, port number, Retry, and Timeout of the primary Geo-Location Server.
  - In the **Secondary Address** and associated **Port**, **Retry** and **Timeout** fields, enter the IPv6 or IPv4 address, port number, Retry, and Timeout of the secondary Geo-Location Server.



**Note** The Maxmind server service supported is GeoIP Legacy web services  
<http://dev.maxmind.com/geoip/legacy/web-services/>.

**Step 6** 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 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.



**Note** If the primary Geo-Location server is shut down and a secondary Geo-location server is configured and is up, requests are sent to the secondary Geo-Location server in a failover-type scenario. If the primary Geo-Location server is brought back up and is online, requests are still routed to the secondary Geo-Location server as long as the secondary Geo-Location server is up. Only if the secondary Geo-Location server goes down and the primary Geo-Location server is up will a fallback occur and requests once again will be routed to the primary Geo-Location server.

## Configuring 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 transaction logs and their formats, see the “[Transaction Logs](#)” section on page 8-54.

To enable transaction logging, follow these steps:

- 
- 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 4-15](#) for a description of the fields.

**Table 4-15** *Transaction Log Settings Fields*

Field	Description
<b>General Settings</b>	
Transaction Log Enable	Enables transaction logging.
Snapshot Counter Log Enable	Enables the Snapshot Counter transaction log. For more information, see the “ <a href="#">Snapshot Counter Transaction Logs</a> ” section on page 8-100.
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</a> ” section on page 8-68.
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	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</a> ” section on page 8-58.
Log Format Custom	Or, choose <b>Log Format Custom</b> and enter a custom format string. For more information, see the “ <a href="#">Custom Format</a> ” section on page 8-61.
<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 4-15** 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.
Skip Log Types	Enables to skip exporting of specific transaction logs. By default, no log type chosen to skip export.
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.
Confirm Password	Confirms the password for the user.

**Table 4-15** Transaction Log Settings Fields (continued)

Field	Description
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.
FTP Export IPv6 Server	IPv6 address or hostname of the FTP 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 8-71.</p>
<b>Web Engine Settings</b>	
Session Log	<p>The Session Log drop-down list has the following options:</p> <ul style="list-style-type: none"> <li>• enable—Enables Session Log for this device, which consists of per-session transaction logging (Per Session logs) and per-fragment transaction logging (Web Engine custom format transaction logs).</li> <li>• enable exclusive—Enables Session Log only for per-session transaction logging.</li> <li>• disable—Disables Session Log.</li> </ul> <p>For more information, see the “<a href="#">Web Engine User Level Session Transaction Logs</a>” section on page 8-96.</p>

**Table 4-15** Transaction Log Settings Fields (continued)

Field	Description
Enable Delivery Service Monitoring	Enables Delivery service Monitoring.
<b>Splunk UF Export Settings</b>	
Export Enable	Enables the automatic export of the selected transaction logs to the designated export server. For more information, see the “Real-Time Exporting of Transaction Logs for Billing and Analytic Reports” section on page 8-102.
Monitors	Check the check boxes of the type of transaction logs to export. The <b>All</b> check box means all transaction logs are exported.
Export Server and Port	IP address and port number of the CDNM, CDN, or other export server that is to receive the transaction log files. A maximum of three export servers can be specified. The default port number is 9998.

**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 Default and Maximum Bandwidth, page 4-34](#)
- [Configuring Bandwidth Schedules, page 4-36](#)
- [Configuring Windows Media Streaming—General Settings, page 4-38](#)
- [Configuring Windows Media Streaming—Bypass List, page 4-40](#)
- [Configuring Movie Streamer—General Settings, page 4-41](#)
- [Configuring RTSP Advanced Settings, page 4-43](#)
- [Configuring Flash Media Streaming—General Settings, page 4-43](#)
- [Configuring Flash Media Streaming—FMS Administrator, page 4-44](#)
- [Configuring Flash Media Streaming—Service Monitoring, page 4-44](#)
- [Configuring Flash Media Streaming—Service Monitoring, page 4-44](#)
- [Configuring Web Engine HTTP Cache Freshness, page 4-45](#)
- [Configuring Tmpfs Size Settings, page 4-46](#)

## 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—General Settings](#)” section on page 4-43 and the “[Configuring Flash Media Streaming—Service Monitoring](#)” section on page 4-44.


**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.”

To configure the default and maximum bandwidth settings, follow these steps:

- 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 4-16](#) for a description of the fields.

**Table 4-16 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. The default is 200 Mbps. <sup>1</sup>
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. The default is 200 Mbps. <sup>1</sup>
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. The default is 200 Mbps. <sup>1</sup>

**Table 4-16 Application Control Default and Maximum Bandwidth Fields (continued)**

Field	Description	
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. The default is 200 Mbps. <sup>1</sup>

1. The maximum bandwidth allowed is 8 Gbps on a CDE220-2G2, 12 Gbps on a, and 44 Gbps on a CDE250.

**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, follow these steps:

- 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 “[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 that you want to edit.
- Step 3** Enter the settings as appropriate. See [Table 4-17](#) for a description of the fields.

**Table 4-17 Application Control Bandwidth Schedule Fields**

Field	Description
Bandwidth Type	Windows Media Incoming—Incoming Windows Media streaming content requests from end users. Windows Media Outgoing—Outgoing Windows Media content from SEs. Movie Streamer Incoming—Incoming Movie Streamer content requests from SEs or origin servers. 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).

**Table 4-17 Application Control Bandwidth Schedule Fields (continued)**

Field	Description
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 page.

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 page. **Table 4-18** describes the view options.

**Table 4-18 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	Toggles between the two options: <ul style="list-style-type: none"> <li>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.</li> <li>Show Effective Bandwidth—Displays the composite (aggregate) bandwidth settings for the SE and its associated device groups.</li> </ul>

**Table 4-18 Viewing Options for Content Services Bandwidth Graph (continued)**

Option	Description
Show Aggregate View/Show Non-Aggregate View	Toggles between the two options: Show Aggregate View—Displays the bandwidth settings configured for the corresponding device groups. Show Non-Aggregate View—Displays the bandwidth settings configured for the SE.
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—General Settings

To configure the General Settings for Windows Media Streaming, follow these steps:

- 
- Step 1** Choose **Devices > Devices > Application Control > Windows Media Streaming > General Settings**. The Windows Media Streaming General Settings page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-19](#) for a description of the fields.

**Table 4-19 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.
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 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.

**Table 4-19 Windows Media Streaming General Settings Fields (continued)**

Field	Description
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 200 sessions. The range is from 1 to 40000.
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). The range is from 1 to 2,147,483,647. The default is 0, which means no bitrate limit.
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. The range is from 1 to 2,147,483,647. The default is 0, which means no bitrate limit.
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.
HTTP Allowed Extensions	List of allowable extensions for HTTP.  You can add or delete filename extensions from this list with the following restrictions: <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 6filename 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>	

**Table 4-19 Windows Media Streaming General Settings Fields (continued)**

Field	Description
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 1000000.
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	The maximum Time to Live for objects in the cache. The value ranges are the following: 1 to 157680000 seconds 1 to 2628000 minutes 1 to 43800 hours 1 to 1825 days 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 Windows Media Streaming—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. This unpredictability is 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, follow these steps:

---

**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 that 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 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, follow these steps:

---

**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 4-20](#) for a description of the fields.

**Table 4-20      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.

**Table 4-20 Movie Streamer General Settings Fields (continued)**

Field	Description
<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 200 sessions. The range is from 1 to 40,000.
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). The range is from 1 to 2147483647, depending on the hardware model.
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. The range is from 1 to 2147483647, depending on the hardware model.
Enable Accelerate VOD Performance	Enables performance improvements in Video On Demand for the Movie Streamer proxy.
<b>Movie Streamer Advanced Client Settings</b>	
Idle Timeout RTP Timeout	<p>The <b>Idle Timeout</b> field and the <b>RTP Timeout</b> field, 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>Idle Timeout</b> field has a range from 0 to 300, whereas the <b>RTP 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 300 for the <b>Idle Timeout</b> field and 180 for the <b>RTP Timeout</b> field.</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> <ul style="list-style-type: none"> <li>1 to 157680000 seconds</li> <li>1 to 2628000 minutes</li> <li>1 to 43800 hours</li> <li>1 to 1825 days</li> </ul> <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 Movie Streamer and Windows Media Streaming, follow these steps:

**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 4-21](#) for a description of the fields.

**Table 4-21 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—General Settings

The Flash Media Streaming engine delivers Adobe Flash applications and video files, as well as MP3 audio files using HTTP and an Adobe proprietary protocol, RTMP. For more information, see the “[Flash Media Streaming Engine](#)” section on page 1-28.



**Note**

Flash Media Streaming uses port 1935 for RTMP and RTMPE streaming. Flash Media Streaming also supports RTMPT and RTMPTE over port 80.

To enable Flash Media Streaming, follow these steps:

**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 4-22](#) for a description of the fields.

**Table 4-22 Flash Media Streaming Fields**

Field	Description
Restricted Maximum Bandwidth	Maximum bandwidth allowed for Flash Media Streaming. The range is from 1000 to 8000000 Kbps. The default is 200000.
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 Flash Media Streaming—FMS Administrator

To enable servers to send Flash Media Server (FMS) Administration API calls to this device, follow these steps:

**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 VDS-IS 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, follow these steps:

**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 configured limitation 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. For more information on memory limitation, see the “[Configuring Memory Limitation Settings](#)” section on page 4-99

**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 HTTP Cache Freshness

To configure the Web Engine HTTP cache freshness, follow these steps:

**Step 1** Choose **Devices > Devices > Application Control > Web > HTTP > HTTP Cache Freshness**. The HTTP Cache Freshness page is displayed (Figure 4-13).

**Figure 4-13** *HTTP Cache Freshness Page*

The screenshot shows the Cisco Content Delivery System Manager interface. The top navigation bar includes links for Home, Logout, System Status (Devices: 4 Devices, Critical; Service: 1 Service, Critical), and tabs for Devices, Services, and System. A sidebar on the left lists various configuration categories like Device Home, Assignments, Replication, Service Control, Application Control (with sub-options for Default and Maximum Bandwidth, Bandwidth Schedules, Windows Media Streaming, Movie Streamer, RTSP Advanced Settings), Web (with sub-options for HTTP, HTTP Connections, HTTP Caching, HTTP Cache Freshness, Advanced HTTP Caching), General Settings, and Monitoring. The main content area is titled "HTTP Cache Freshness Settings" and displays "Current applied settings from Service Engine, NE-612-5". It contains several input fields: "Enable" (checkbox), "Object Age Multiplier" (text box with value 30), "Max TTL Scale" (dropdown menu set to "days"), "Max Object TTL" (text box with value 1), "Minimum TTL" (text box with value 80, followed by "(Minutes)"), and "Enable Re-evaluate Request All" (checkbox). A note at the bottom states "Note: \* - Required Field". At the bottom right are "Submit" and "Cancel" buttons. The page is identified by the ID 211810.

**Step 2** Enter the settings as appropriate. See Table 4-23 for a description of the fields.

**Table 4-23** *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.

**Table 4-23 HTTP Cache Freshness Fields (continued)**

Field	Description
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.
Max Object TTL	The maximum Time to Live (TTL) for objects in cache. The ranges are as follows: 1 to 1825 days 1 to 43800 hours 1 to 2628000 minutes 1 to 157680000 seconds The default is 61 day.
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.

**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 Tmpfs Size Settings

To configure the Tmpfs size settings, follow these steps:

**Step 1** Choose **Devices > Devices > Application Control > Web > HTTP > Tmpfs Size**. The Tmpfs size settings page is displayed.

**Step 2** In the **tmpfs-size** field, enter the percentage of physical memory. The default is 25 percent. The range is from 10 to 90 percent.

**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.

## General Settings

The General Settings pages provide settings for access control of the device, maintenance, network connectivity, and monitoring. The configuring of general settings consists of the following procedures:

- [Configuring Content Management, page 4-47](#)
- [Login Access Control, page 4-49](#)
- [Authentication, page 4-56](#)
- [Scheduling Database Maintenance, page 4-60](#)

- [Setting Storage Handling, page 4-61](#)
- [Network Settings, page 4-63](#)
- [Configuring Notification and Tracking, page 4-81](#)
- [Configuring Troubleshooting, page 4-97](#)
- [Configuring Service Router Settings, page 4-98](#)
- [Configuring Cache Router Settings, page 4-98](#)
- [Configuring Memory Limitation Settings, page 4-99](#)

## Configuring Content Management

To configure the maximum number of entries for cache content, follow these steps:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Devices &gt; Devices &gt; General Settings &gt; Content Management</b> . The Content Management page is displayed. |
| <b>Step 2</b> | Enter the settings as appropriate. See <a href="#">Table 4-24</a> for a description of the fields.                           |

**Table 4-24 Content Management Fields**

Field	Description
Max Cache Content Entries	<p>Enter the value for the maximum entries of cached content allowed.</p> <ul style="list-style-type: none"> <li>• The maximum cached file entries is 20 million for a platform with physical memory size less than 32GB(33,554,432KB). The default is 16 million.</li> </ul> <p>If you enter the value more than 20 million for maximum cached files entries, and click <b>Submit</b>, only the maximum value that is 20 million is applied on the SE.</p> <p>For more information, see the <i>Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference Guide</i>.</p> <ul style="list-style-type: none"> <li>• The maximum cached file entries is 50 million for a platform with physical memory size more than 32GB(33,554,432KB). The default is 40 million.</li> </ul>
Max Cache Content Directories	<p>Enter the value for the maximum directories of cached content allowed.</p> <ul style="list-style-type: none"> <li>• The maximum cached file directories is 1 million for a platform with physical memory size less than 32GB(33,554,432KB). The default is 800,000.</li> </ul> <p>If you enter the value more than 1 million for the maximum cached file directories and click <b>Submit</b>, only the maximum value that is 1 million is applied on the SE.</p> <p>For more information, see the <i>Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference Guide</i>.</p> <ul style="list-style-type: none"> <li>• The maximum cached file directories is 10 million for a platform with physical memory size more than 32GB(33,554,432KB). The default is 8 million.</li> </ul>

**Table 4-24 Content Management Fields (continued)**

Field	Description
Cache content eviction preferred size	By default, Content Manager prefers to keep small content objects over large content objects, because the overhead of fetching a small object is higher than larger objects. The <b>Cache content eviction preferred size</b> default is large, which means the large size files are evicted before small files.
Enable Small Content Eviction Protection	Check the <b>Enable Small Content Eviction Protection</b> check box, to enable small content eviction protection. For more information, see the “ <a href="#">Eviction Protection</a> ” section on page 1-11.
Maximum small cache entry size to protect	From the <b>Maximum small cache entry size to protect</b> drop-down list, choose the maximum cache entry size (500 KB, 1 MB, 2 MB, 4 MB, 10 MB, and 20 MB) to protect from deletion.
Minimum duration to protect the small content from eviction	From the <b>Minimum duration to protect the small content from eviction</b> drop-down list, choose the age (5-30 mins) of the content object to be protected from deletion.
Enable Large Content Eviction Protection	Check the <b>Enable Large Content Eviction Protection</b> check box to enable eviction protection. For more information, see the “ <a href="#">Eviction Protection</a> ” section on page 1-11.
Minimum large cache entry size to protect	From the <b>Minimum large cache entry size to protect</b> drop-down list, choose the minimum cache entry size (100 MB, 500 MB, 1 GB, and 4 GB) to protect from deletion.
Minimum duration to protect the large content from eviction	From the <b>Minimum duration to protect the large content from eviction</b> drop-down list, choose the age (1-4 hours for 100 MB size, 1, 4, 8, or 24 hours for all other sizes) of the content object to be protected from deletion.
Hit Count Decay Half Life	Enter the half-life decay period (in days) at which to decay hit-count by half. The range is 1 to 30. The default is 14 days. The decay mechanism reduces the hit count by half and is applied for the content object every two weeks by default.
Threshold of Disk Failures Per Bucket	Enter the threshold, as a percentage, for disk failures in a bucket. The disks in each bucket are monitored, and if the threshold is exceeded, a minor alarm is raised. The default is 30. The range is 1 to 100. For more information, see the “ <a href="#">Bucket Allocation</a> ” section on page 1-7.
Primary start-time of slowscan	The slowscan runs at this time every day. In default, it is "00:00".
Secondary start-time of slowscan	The slowscan runs at this time either. With such configuration, slowscan runs twice every day. By default, it is not set.

**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.

## 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 a VDS-IS 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 6-1.

### Login Authentication

Login authentication provides the configuration for independent logins; in other words, 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.



If you plan to use a RADIUS server or a TACACS+ server for authentication, you must configure the server settings before you configure and submit these settings. See the “[Configuring RADIUS Server Settings](#)” section on page 4-56 and the “[Configuring TACACS+ Server Settings](#)” section on page 4-57 for more information.

When the primary login server and the primary enable 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.



If the **Enable Failover Server Unreachable** option is enabled, it applies to both the login authorization methods and the exec authentication methods.

If you are going to use different servers for login authentication and enable authentication (for example, local for login authentication and RADIUS for the enable authentication), then the username and password must be the same for both servers.

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.”

**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.

To configure the login authentication and enable authentication schemes for the device, follow these steps:

- Step 1** Choose **Devices > Devices > General Settings > Login Access Control > Login Authentication**. The Login Authentication page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-25](#) for a description of the fields.

**Table 4-25      Login Authentication Fields**

Field	Description
<b>Login Authentication Settings</b>	
Enable Failover Server Unreachable	<p>If <b>Enable Failover Server Unreachable</b> is enabled, the following applies:</p> <ul style="list-style-type: none"> <li>• Only two login authentication schemes (a primary and secondary scheme) are allowed on the device.</li> <li>• Device fails over from the primary authentication scheme to the secondary authentication scheme only if all specified authentication servers of the primary authentication scheme are unreachable.</li> </ul> <p>Conversely, if the <b>Enable Failover Server Unreachable</b> option is disabled, the device contacts the secondary authentication database, regardless of the reason the authentication failed with the primary authentication database.</p> <p><b>Note</b> To use this option, you must set TACACS+ or RADIUS as the primary authentication method and local as the secondary authentication method.</p>
Authentication Login Servers	<p>When enabled, login authentication servers are used to authenticate user logins and whether the user has access permissions to the device.</p> <p>Check this option and set one or more Login servers for login authentication. By unchecking this option, local authentication is used by default. Three servers can be configured.</p> <p><b>Note</b> If local is selected for any of the Login servers, the password in the username is used to authenticate the user. See the “<a href="#">Creating, Editing, and Deleting Users—Usernames</a>” section on page 4-55.</p>
Primary Login Server	Choose local, RADIUS, or TACACS+.
Secondary Login Server	Choose local, RADIUS, or TACACS+.
Tertiary Login Server	Choose local, RADIUS, or TACACS+.
<b>Enable Authentication Settings</b>	
Primary Enable Server	The enable server is used to allow normal users to enter the privileged EXEC mode. Choose local, RADIUS, or TACACS+.
Secondary Enable Server	Choose local, RADIUS, or TACACS+.

**Table 4-25 Login Authentication Fields (continued)**

Field	Description
Tertiary Enable Server	Choose local, RADIUS, or TACACS+.
Local Enable Password	Set the local enable password for normal users to log in to the Enable server and have privileged EXEC mode. If multiple authorization methods are configured, the SE tries to authenticate the enable password by way of each configured method until one of them is successful.

**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.

---

## Exec Authorization

Exec authorization provides the configuration for determining the services allowed for each user that logs in to the device.

Exec authorization can also be used to determine the services the user has for 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 TACACS+ server for authorization, you must configure the server settings before you configure and submit these settings. See the “Configuring RADIUS Server Settings” section on page 4-56 and the “Configuring TACACS+ Server Settings” section on page 4-57 for more information.

---

When the primary authorization server is set to local, usernames and passwords are local to each device. Local authorization uses locally configured login and passwords to authorize services for the user.



### Note

If the **Enable Failover Server Unreachable** option is enabled, it applies to both the login authorization methods and the exec authentication methods.

If you are going to use different servers for login authentication and enable authentication (for example, local for login authentication and RADIUS for the enable authentication), then the username and password must be the same for both servers.

---



### 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.

---

To configure the exec authorization schemes for the device, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Login Access Control > Exec Authorization**. The Exec Authorization page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-26](#) for a description of the fields.

**Table 4-26 Exec Authorization Fields**

Field	Description
Authorization Exec Servers	When enabled, authorization exec servers are used to authorize services for logged in users.  Check this option and set one or more servers for exec authorization. By unchecking this option, local authentication is used by default. Three servers can be configured.  <b>Note</b> If a user encounters failure during EXEC shell) startup authorization, the user fails to log in to the SE even if the user passed the login authentication.
Primary Exec Server	Choose local, RADIUS, or TACACS+.
Secondary Exec Server	Choose local, RADIUS, or TACACS+.
Tertiary Exec Server	Choose local, RADIUS, or TACACS+.
Primary Enable Server	The enable server determines if the normal user can enter the privileged EXEC mode. Choose local, RADIUS, or TACACS+.
Normal User Commands	Choose <b>Enable</b> or <b>Enable if Authenticated</b> .  The <b>Enable if Authenticated</b> option turns off authorization on the TACACS+ server and authorization is granted to any Normal user who is authenticated.
Super User Commands	Choose <b>Enable</b> or <b>Enable if Authenticated</b> .  The <b>Enable if Authenticated</b> option turns off authorization on the TACACS+ server and authorization is granted to any Super user who is authenticated.
Enable Config Commands	Check the <b>Enable Config Commands</b> check box to enable authorization of the configuration mode commands.  By default, this option is disabled, which means all configuration commands issued are allowed.
Enable Console Config	Check the <b>Enable Console Commands</b> check box to enable authorization of all commands issued on a console TTY connection.  By default, this option is disabled, which means commands issued through a console TTY connection always succeed.



**Note** The following commands bypass authorization and accounting: CTRL+C, CTRL+Z, **exit**, **end**, and all of configuration commands for entering submode (for example, **interface GigabitEthernet 1/0**).

- 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 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, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Login Access Control > SSH**. The SSH page is displayed.
- Step 2** Check **Enable** to enable the SSH feature. SSH enables login access to the device through a secure and encrypted channel.
- Step 3** In the **Length of Key** field, specify the number of bits needed to create an SSH key. The default is 2048.
- Step 4** In the **Login Grace Time** field, specify the number of seconds that 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 5** Select the SSH version.
- To allow clients to connect using SSH protocol version 1, check the **Enable SSHv1** check box.
  - 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 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 Telnet

To enable the Telnet service, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Login Access Control > Telnet**. The Telnet page is displayed.

**Step 2** Check **Telnet Enable** to enable the terminal emulation protocol for remote terminal connections.

**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.

---

## 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, follow these steps:

**Step 1** Choose **Devices > Devices > General Settings > Login Access Control > Message of the Day**. The MOTD page is displayed.

**Step 2** 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 3** 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 4** 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 5** 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 6** Check the **Device Mode Display Enable** check box to enable device mode display.

**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.

---

## Changing the CLI Session Time

To change the CLI session time, follow these steps:

**Step 1** Choose **Devices > Devices > General Settings > Login Access Control > CLI Session Time**. The CLI Session Time page is displayed.

**Step 2** In the **CLI Session Time** field, enter the time (in minutes) that the device waits for a response before ending the session.

**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.

---

## 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 VDS-IS. 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, follow these steps:

**Step 1** Choose **Devices > Devices > General Settings > Login Access Control > Users > Admin Password**. The Admin Password page is displayed.

**Step 2** In the **Password** field, enter a new password.

The following characters are not allowed: ?./;[]{}"=@=

**Step 3** In the **Confirm Password** field, re-enter the password.

**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.

---

## 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, follow these steps:

**Step 1** Choose **Devices > Devices > 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 “[Aggregate Settings](#)” section on page 4-8

**Step 2** 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 that you want to edit.

**Step 3** Enter the settings as appropriate. See [Table 4-27](#) for a description of the fields.

**Table 4-27 Local User Fields**

Field	Description
Username	Name of user.
Password	User password.
Confirm Password	Re-enter user password.
Privilege	<p>There are two types of predefined privilege profiles:</p> <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 4** 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.

## Configuring RADIUS Server Settings



**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, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Authentication > RADIUS Server**. The RADIUS Server Settings page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-28](#) for a description of the fields.

**Table 4-28 RADIUS Server Settings Fields**

<b>Field</b>	<b>Description</b>
Enable Radius Authentication	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.
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. <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 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.

To use RADIUS for login authentication and authorization, see the “[Login Authentication](#)” section on [page 4-49](#).

## Configuring TACACS+ Server Settings



**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.

To configure the TACACS+ server settings, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Authentication > TACACS+ Server**. The TACACS+ Server Settings page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-29](#) for a description of the fields.

**Table 4-29 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.
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. The range is from 1 to 99. An empty string is the default.
Primary Server	IP address or hostname of the primary TACACS+ server.
Secondary Server	IP address or hostname of the backup TACACS+ server. Up to two backup servers are allowed.
Tertiary Server	

**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.

To use TACACS+ for login authentication and authorization, see the “[Login Authentication](#)” section on [page 4-49](#).

## Configuring AAA Accounting

Accounting tracks all user actions and when the action occurred. It can be used for an audit trail or for billing for connection time or resources used (bytes transferred).

The VDS-IS accounting feature uses TACACS+ server logging. Accounting information is sent to the TACACS+ server only, not to the console or any other device. The syslog file on the SE logs accounting events locally. The format of events stored in the syslog is different from the format of accounting messages.

The TACACS+ protocol allows effective communication of AAA information between SEs and a central TACACS+ server. It uses TCP for reliable connections between clients and servers. SEs send authentication and authorization requests, as well as accounting information to the TACACS+ server.



**Note** Before you can configure the AAA accounting settings for a device, you must first configure a TACACS+ server for the device. See the “[Configuring TACACS+ Server Settings](#)” section on [page 4-57](#).

**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.

To configure the AAA accounting settings, follow these steps:

- Step 1** Choose **Devices > Devices > General Settings > Authentication > AAA Accounting**. The AAA Accounting Settings page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-29](#) for a description of the fields.

**Table 4-30 AAA Accounting Settings Fields**

Field	Description
System Events	<p>Enables accounting records on the TACACS+ server about system events; such as system reboot, interface up or down states, and accounting configuration enabled or disabled.</p> <p>From the <b>System Events</b> drop-down list, choose <b>start-stop</b> or <b>stop-only</b>.</p> <p>The <b>start-stop</b> option records events when they start and when they stop. The <b>stop-only</b> option records events when they stop.</p>
Exec Shell Events	<p>Enables accounting records on the TACACS+ server about user EXEC terminal sessions, including username, date, and start and stop times.</p> <p>From the <b>Exec Shell Events</b> drop-down list, choose <b>start-stop</b> or <b>stop-only</b>.</p> <p>The <b>start-stop</b> option records events when they start and when they stop. The <b>stop-only</b> option records events when they stop.</p>
Normal User Commands	<p>Enables accounting records on the TACACS+ server for Normal users using commands in the EXEC mode.</p> <p>From the <b>Normal User Commands</b> drop-down list, choose <b>start-stop</b> or <b>stop-only</b>.</p> <p>The <b>start-stop</b> option records events when they start and when they stop. The <b>stop-only</b> option records events when they stop.</p>
Super User Commands	<p>Enables accounting records on the TACACS+ server for Super users using commands in the EXEC mode.</p> <p>From the <b>Super User Commands</b> drop-down list, choose <b>start-stop</b> or <b>stop-only</b>.</p> <p>The <b>start-stop</b> option records events when they start and when they stop. The <b>stop-only</b> option records events when they stop.</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 an Access Control List

To configure an access control list (ACL) for group authorization, follow these steps:

- 
- Step 1** Choose **Devices > Devices > 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 2** 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 that you want to edit.
- Step 3** Enter the settings as appropriate. See [Table 4-31](#) for a description of the fields.

**Table 4-31 Access Control List Fields**

Field	Description
Action	Whether to permit or deny access for this group.
Group Name	If this action is for all groups, choose <b>Any Group Name</b> . 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 4** 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 5** From the left-panel menu, choose **Enable Access Control List**. The Enable Access Control List page is displayed.
- Step 6** 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:

- The last vacuum process happened more than 30 minutes in the past.
- The percent increase in disk space usage is greater than 10 percent.
- The 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 re-indexing, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Database Maintenance**. The Database Maintenance Settings page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-32](#) for a description of the fields.

**Table 4-32 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 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.

---

## Setting Storage Handling

The Storage option offers disk error-handling settings.

### Enabling Disk Error Handling

The Disk Error Handling page allows you to configure how disk errors are handled, and to define disk error-handling thresholds for bad sectors and disk errors (I/O errors).

The **Threshold for Bad Sectors** and the **Threshold for Disk Errors** counts only apply to bad sectors and disk errors detected since the last reboot of the device. These counts do not persist across a device reboot (reload).

If the **Enable Disk Error Handling Reload** option is enabled and a SYSTEM disk drive is marked bad because the disk error-handling threshold (bad sectors or disk errors) was reached, the device is automatically reloaded. Following the device reload, the bad sector and disk error threshold counts are reset, and a syslog message and an SNMP trap are generated.

If a critical disk drive is marked bad, the redundancy of the system disks for this device is affected. Critical disks are disks with SYSTEM partitions. However, drives with SYSTEM partitions use RAID1. With the RAID system, if the critical primary disk fails, the other mirrored disk (mirroring only occurs for SYSTEM partitions) seamlessly continues operation. There is a separate alarm for bad RAID. The SMART statistics that are returned by the **show disks SMART-info detail** command include sector errors directly reported by the drive itself.

For more information about the SMART sector errors, latent sector handling, and the **disk repair** command, see the “[Disk Maintenance](#)” section on page 9-27.



**Note** We do not recommend enabling the **Enable Disk Error Handling Reload** option, because the software state may be lost when the device is reloaded.

To configure a disk error-handling method, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Storage > Disk Error Handling**. The Disk Error Handling Settings page is displayed.
  - Step 2** Check the **Enable** check box.
  - Step 3** Check the **Enable Disk Error Handling Reload** check box if you want the device to reload when a critical disk (SYSTEM) has problems.
  - Step 4** 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 bad, and enter the following:
    - a. In the **Threshold for Bad Sectors** field, enter the number of allowed bad sectors before marking the disk bad. This threshold only applies to bad sectors detected since the last reboot of the device. The range is 0 to 100. The default threshold is 30.
    - b. In the **Threshold for Disk Errors** field, enter the number of allowed disk errors (I/O errors) before marking the disk bad. This threshold only applies to disk and sector errors detected since the last reboot of the device. The range is from 0 to 100,000. The default is 500.



**Note** When both **Threshold for Bad Sectors** and **Threshold for Disk Errors** are set to 0, it means never mark the disk bad when it detects bad sectors or disk errors, and the **disk\_failure** alarm is not raised. A disk with SYSTEM partitions uses RAID1. There is a separate alarm for bad RAID.

- 
- 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.

---

When a sector I/O error is detected, a “badsector” alarm is raised against the corresponding disk, which occurs during the lifetime of a disk. A “badsector” alarm is raised when the number of bad sectors for a specific disk exceeds the “badsector” alarm threshold. The default threshold for bad sector alarms is set to 15 errored sectors. See the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference* for information on setting the threshold for bad sector alarms and remapped sector alarms, by using the following commands:

```
(config)# disk error-handling threshold alarm-bad-sectors <threshValue>
(config)# disk error-handling threshold alarm-remapped-sectors <threshValue>
(config)# disk error-handling bad-sectors-mon-period <minutes>
```

The **Disk Failure Percentage Threshold** field in the Service Monitor page sets the overall percentage of CDNFS disk failures. When the percentage of failed disks (default is 75) exceeds this threshold, no further requests are sent to this device. The **Disk Failure Threshold** setting is only for the CDNFS disks. For more information, see the “[Setting Service Monitor Thresholds](#)” section on page 4-83.

## Network Settings

The Network pages provide settings for network connectivity. Configuring network settings consist of the following procedures:

- [Enabling FTP Services, page 4-63](#)
- [Enabling DNS, page 4-63](#)
- [Enabling RCP, page 4-64](#)
- [Configuring NTP, page 4-64](#)
- [Configuring TCP, page 4-65](#)
- [Setting the Time Zone, page 4-65](#)
- [Viewing Network Interfaces, page 4-68](#)
- [Configuring External IP Addresses, page 4-68](#)
- [Configuring Port Channel and Load Balancing Settings, page 4-69](#)
- [Configuring IP General Settings, page 4-70](#)
- [Configuring IP ACL for IPv4 and IPv6, page 4-70](#)
- [Configuring Static Routes, page 4-79](#)
- [Configuring Static IPv6 Routes, page 4-80](#)
- [Configuring DSR VIP, page 4-80](#)

### Enabling FTP Services

To enable FTP services to listen for connection requests, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > FTP**. The FTP Settings page is displayed.
- Step 2** Check the **Enable FTP Services** check box.
- 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.

---

### 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, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > DNS**. The DNS Settings page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-33](#) for a description of the fields.

**Table 4-33 DNS Settings Fields**

Field	Description
Enable	Enables Domain Name System (DNS) on the device.
List of DNS Servers	Space-delimited list of IPv6 or IPv4 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 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.

---

## 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, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > RCP**. The RCP page is displayed.
- Step 2** Check the **RCP Enable** check box to have the RCP services listen for RCP requests.
- 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 NTP

To configure the device to synchronize its clock with an NTP server, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > NTP**. The NTP page is displayed.
- Step 2** Check **Enable** to enable NTP.

**Step 3** In the **NTP Server** field, enter the IPv6 or IPv4 address or hostname of up to four NTP servers. Use a space to separate the entries.

**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 TCP

To configure the TCP settings for service engine, follow these steps:

**Step 1** Choose **Devices > Devices > General Settings > Network > TCP**. The TCP page is displayed.

**Step 2** Check **Enable TCP Timestamps** to enable TCP timestamps. By default, it is enabled.

**Step 3** Check **Enable fast recycling of TIME-WAIT sockets** to set **tcp\_tw\_recycle** parameter. By default, it is enabled.

**Step 4** Check **Enable safe reusing of TIME-WAIT sockets** to set **tcp\_tw\_reuse** parameter. By default, it is enabled.

**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.

## 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 VDS-IS 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, follow these steps:

**Step 1** Choose **Devices > Devices > 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 2** To configure a standard time zone, follow these steps:

- 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 4-34 on page 4-67](#).

- 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 3** To configure a customized time zone, follow these steps:
- a. Click the **Customized Time Zone** radio button.
  - b. In the **Customized Time Zone** field, enter a name to 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 4** To configure customized summer time savings, follow these steps:



**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 choose 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 5** 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 6** In the **Offset** field, specify the minutes offset from UTC (0 to 1439). (See [Table 4-34 on page 4-67](#).)

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 7** To not specify a summer or daylight savings time for the corresponding time zone, click the **No Customized Summer Time Configured** radio button.

**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.

---

Table 4-34 lists the UTC offsets for the different locations around the world.

**Table 4-34 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
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

**Table 4-34 Time Zone—Offset from UTC (continued)**

Time Zone	Offset from UTC (in hours)	Time Zone	Offset from UTC (in hours)
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.

Starting with Release 3.3, VDS-IS supports assigning multiple IP address in different subnets on a port channel.



**Note** The **loopback address** configuration feature is supported starting with Release 3.3.

The loopback address is a single usable IP address in a network. In some CDN deployment, it is required to configure a loopback address for traffic and management interfaces to hide the interconnection addresses of the CDN to the client. There are 2 addresses per interface:

- port-channel or single link
- loopback

The 32-bit subnet mask is used to configure a loopback address. Because the 32-bit subnet mask is not allowed in the current release. To apply a loopback address from the CLI, use the following interface configuration command:

```
(config)#interface gigabitEthernet 1/0 ip address 1.1.1.1 255.255.255.255 secondary
```

After the loopback ip address is assigned, the interface can be configured as a streaming interface to serve the streaming, or as the management interface for internal communication.

## Configuring External IP Addresses

The External IP page allows you to configure up to eight Network Address Translation (NAT) IP address. 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, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > External IP**. The External IP Settings page is displayed.
- Step 2** Check the **Enable** check box.
- Step 3** In the External IP address fields (1–8), enter up to eight IP addresses.
- 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 Port Channel and Load Balancing Settings

For information about configuring port channels using the CLI, see the “[Redundant Dedicated Management Ports](#)” section on page I-6.

To configure load balancing on port channels, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > Port Channel Settings**. The Port Channel Settings page is displayed.
- Step 2** 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-mixed-ip-port**—Destination IP address and TCP/UDP port
  - **dst-port**—Destination port
  - **round robin**—Each interface in the channel group
  - **src-dst-ip**—Source and destination IP address
  - **src-dst-mac**—Source and destination MAC address
  - **src-dst-mixed-ip-port**—Source destination IP address and source destination port
  - **src-dst-port**—Source and destination port
  - **src-mixed-ip-port**—Source IP address and source 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 mean that while calculating the outgoing interface, take into account both the source and destination (MAC address or port).



**Note** Round-robin load-balancing mode is not supported when Link Aggregation Control Protocol (LACP) is enabled on the port channel.

---

- 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 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, follow these steps:

- Step 1** Choose **Devices > Devices > General Settings > Network > IP General Settings**. The IP General Settings page is displayed.
- Step 2** Check **Enable Path MTU Discovery**.
- 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 IP ACL for IPv4 and IPv6

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.



**Note** ACLs for IPv6 are separate from IPv4. To create IP ACLs for IPv4, choose **Devices > Devices > General Settings > Network > IP ACL**. To create IP ACLs for IPv6, choose **Devices > Devices > General Settings > Network > IPv6 ACL**.

---

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 VDS-IS network environment, administrators need to be able to prevent unauthorized access to various devices and services. VDS-IS supports standard and extended ACLs that allow administrators to restrict access to or through a VDS-IS 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 VDSM 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.
- Device is deployed as a reverse proxy in an untrusted environment, and the administrator wishes to allow only port 80 inbound traffic on the outside interface and outbound connections on the back-end interface.

**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 non-numeric characters.
- Extended IP ACLs cannot be used with SNMP applications.

### Creating a New IP ACL

To create a new IP ACL, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > IP ACL** for IPv4 addressing. Choose **Devices > Devices > General Settings > Network > IPv6 ACL** for IPv6 addressing. The IP ACL Table page is displayed.  
The table is sortable by clicking the column headings.
- Step 2** 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 that you want to edit.
- Step 3** In the **Name** field, enter a name, observing the naming rules for IP ACLs.
- Step 4** From the **ACL Type** drop-down list, choose an IP ACL type (**Standard** or **Extended**). The default is **Standard**.
- Step 5** 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, follow these steps:

- Step 1** Choose **Devices > Devices > General Settings > Network > IP ACL** for IPv4 addressing. Choose **Devices > Devices > General Settings > Network > IPv6 ACL** for IPv6 addressing. The IP ACL Table page is displayed.
- Step 2** 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 3** 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 that 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 4** 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 5](#).
  - To create an extended IP ACL, go to [Step 6](#).
- Step 5** To set up conditions for a standard IP ACL, follow these steps:
  - 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 4-35](#) describes the fields in a standard IP ACL.

**Table 4-35 Standard IP ACL Conditions**

Field	Default Value	Description
Purpose <sup>1</sup>	Permit	Specifies whether a packet is to be passed ( <b>Permit</b> ) or dropped ( <b>Deny</b> ).
Source IP <sup>1</sup>	0.0.0.0	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 IPv6	0::0	for IPv4.
Source IP <sup>1</sup> 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 for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Source Prefix	0	

1. Required field.

**Step 6** To set up conditions for an extended IP ACL, follow these steps:

- From the **Purpose** drop-down list, choose a purpose (**Permit** or **Deny**).
- 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.
- Enter the settings as appropriate. See [Table 4-36](#) for descriptions of the extended IP ACL fields.
- Click **Submit**. The Modifying IP ACL page is displayed showing the new condition and its configuration.
- To add another condition to the IP ACL, repeat the steps.
- 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.

- 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 4-36 Extended IP ACL Conditions**

Field	Default Value	Description	Extended Type
Purpose <sup>1</sup>	Permit	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

**Table 4-36 Extended IP ACL Conditions (continued)**

Field	Default Value	Description	Extended Type																						
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 <sup>1</sup>	0.0.0.0	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 for IPv4.	Generic, TCP, UDP, ICMP																						
SourceIPv6	0::0																								
Source IP Wildcard <sup>1</sup>	255.255.255.255		Generic, TCP, UDP, ICMP																						
Source Prefix	0	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.																							
Source Port 1	0	<p>Decimal number or name of a port. Valid port numbers are 0 to 65535. See <a href="#">Table 4-37</a> and <a href="#">Table 4-38</a> for port name descriptions and associated port numbers.</p> <table> <tr> <td>Valid TCP port names are as follows:</td> <td>Valid UDP port names are as follows:</td> </tr> <tr> <td>• domain</td> <td>• bootpc</td> </tr> <tr> <td>• exec</td> <td>• bootps</td> </tr> <tr> <td>• ftp</td> <td>• domain</td> </tr> <tr> <td>• ftp-data</td> <td>• netbios-dgm</td> </tr> <tr> <td>• https</td> <td>• netbios-ns</td> </tr> <tr> <td>• nfs</td> <td>• netbios-ss</td> </tr> <tr> <td>• rtsp</td> <td>• nfs</td> </tr> <tr> <td>• ssh</td> <td>• ntp</td> </tr> <tr> <td>• telnet</td> <td>• snmp</td> </tr> <tr> <td>• www</td> <td>• snmptrap</td> </tr> </table>	Valid TCP port names are as follows:	Valid UDP port names are as follows:	• domain	• bootpc	• exec	• bootps	• ftp	• domain	• ftp-data	• netbios-dgm	• https	• netbios-ns	• nfs	• netbios-ss	• rtsp	• nfs	• ssh	• ntp	• telnet	• snmp	• www	• snmptrap	TCP, UDP
Valid TCP port names are as follows:	Valid UDP port names are as follows:																								
• domain	• bootpc																								
• exec	• bootps																								
• ftp	• domain																								
• ftp-data	• netbios-dgm																								
• https	• netbios-ns																								
• nfs	• netbios-ss																								
• rtsp	• nfs																								
• ssh	• ntp																								
• telnet	• snmp																								
• www	• snmptrap																								
Source Operator	range	Specifies how to compare the source ports against incoming packets. Choices are <, >, ==, !=, or range.	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		Generic, TCP, UDP, ICMP																						
Destination IPv6	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 for IPv4.																							
Destination IP Wildcard	255.255.255.255		Generic, TCP, UDP, ICMP																						
Destination Prefix	0	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.																							

**Table 4-36 Extended IP ACL Conditions (continued)**

Field	Default Value	Description	Extended Type
Destination Port 1	0	<p>Decimal number or name of a port. Valid port numbers are 0 to 65535. See <a href="#">Table 4-37</a> and <a href="#">Table 4-38</a> for port name descriptions and associated port numbers.</p> <p>Valid TCP port names are as follows:</p> <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> <p>Valid UDP port names are as follows:</p> <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>	TCP, UDP
Destination Operator	range	Specifies how to compare the destination ports against incoming packets. Choices are <, >, ==, !=, or range.	TCP, UDP
Destination Port 2	65535	Decimal number or name of a port. See Destination Port 1.	TCP, UDP
ICMP Param Type <sup>1</sup>	None	Choices are <b>None</b> , <b>Type/Code</b> , or <b>Msg</b> .	ICMP
ICMPv6 Param Type		<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>	
ICMP Message <sup>1</sup>	administratively-prohibited	Allows a combination of ICMP type and code to be specified using a keyword chosen from the drop-down list.	ICMP
ICMPv6 Message		See <a href="#">Table 4-39</a> for descriptions of the ICMP messages.	
ICMP Type <sup>1</sup>	0	Number from 0 to 255. This field is enabled when you choose <b>Type/Code</b> .	ICMP
ICMPv6 Type			
Use ICMP Code <sup>1</sup>	Unchecked	When checked, enables the ICMP Code field.	ICMP
Use ICMPv6 Code			
ICMP Code <sup>1</sup>	0	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
ICMPv6 Code			

1. Required field.

[Table 4-37](#) lists the UDP keywords that you can use with extended access control lists.

**Table 4-37 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 4-38](#) lists the TCP keywords that you can use with extended access control lists.

**Table 4-38 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 4-39](#) lists the keywords that you can use to match specific ICMP message types and codes.

**Table 4-39 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.

**Table 4-39      Keywords for ICMP Message Type and Code (continued)**

<b>Message</b>	<b>Description</b>
dod-net-prohibited	Messages that specify a DoD protocol network denial.
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.

**Table 4-39** Keywords for ICMP Message Type and Code (continued)

Message	Description
protocol-unreachable	Messages that specify that the protocol is unreachable.
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 {GigabitEthernet | Portchannel | Standby | TenGigabitEthernet} slot/port [ip | IPv6]
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, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > IP ACL** for IPv4 addressing. Choose **Devices > Devices > General Settings > Network > IPv6 ACL** for IPv6 addressing. The IP ACL Table page is displayed.
- Step 2** 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 of the conditions, while preserving the IP ACL name.
  - **Delete IP ACL Condition**—This option removes one condition from the ACL.
- Step 3** 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 4** To delete only the conditions, click **Delete All Conditions** in the task bar. You are prompted to confirm your action. Click **OK**. The page refreshes, conditions are deleted, and the ACL Type field becomes available.
- Step 5** To delete one condition, follow these steps:
  - 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.
- 

## Configuring Static Routes

The Static IP Routes page allows you to configure a static IPv4 route for a network or host. Any IP packet designated for the specified destination uses the configured route.

To configure a static IP route, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > Static IP Routes**. The IP Route Table page is displayed.
- The table is sortable by clicking the column headings.
- Step 2** 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 that you want to edit.
- Step 3** In the **Destination Network Address** field, enter the destination network IP address.
- Step 4** In the **Netmask** field, enter the destination host netmask.
- Step 5** In the **Gateway's IP address** field, enter the IP address of the gateway interface.
- Step 6** 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 Static IPv6 Routes

The Static IPv6 Routes page allows you to configure a static IPv6 route for a network or host. Any IP packet designated for the specified destination uses the configured route.

To configure a static IPv6 route, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > Static IPv6 Routes**. The IPv6 Route Table page is displayed.  
The table is sortable by clicking the column headings.
- Step 2** Click the **Create New** icon in the task bar. The IPv6 Route page is displayed.  
To edit a static route, click the **Edit** icon next to the name that you want to edit.
- Step 3** In the **Destination Network Address** field, enter the destination network IPv6 address.
- Step 4** In the **Prefix** field, enter the prefix length of the route, subnet, or address range. For example, for 2001:DB8::/32, the prefix length is 32.
- Step 5** In the **Gateway's IPv6 Address** field, enter the IPv6 address of the gateway interface.
- Step 6** 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 VDS-IS 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 VDS-IS 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 VDS-IS (and supported on the load balancer), all VDS-IS responses to the client are sent directly to the client, bypassing the load balancer.



- 
- Note** If DSR VIP is configured on an SE, the DSR VIP IP address cannot be the same as the Origin Server FQDN (OFQDN).

To configure a DSR VIP, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Network > DSR VIP**. The DSR VIP page is displayed.
- Step 2** In the **Direct Server Return VIP 1** field, enter the IPv4 address of the Direct Server Return VIP. In the **Direct Server Return IPv6 VIP1** field, enter the IPv6 address of the Direct Server Return VIP.
- Step 3** Enter any additional DSR VIPs in the remaining fields (Direct Server Return [IPv6] VIP 2 to 4).
- 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 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 Overload Detection, page 4-81](#)
- [Setting Service Monitor Thresholds, page 4-83](#)
- [Enabling System Monitor Settings, page 4-87](#)
- [Configuring SNMP, page 4-88](#)
- [Enabling System Logs, page 4-96](#)

### Alarm Settings

The Alarm Settings page covers the following configuration settings:

- [Enabling Alarm Overload Detection, page 4-81](#)
- [Alarms for Admin Shutdown Interface, page 4-82](#)

#### Enabling Alarm Overload Detection

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 4-40](#). These CLI commands allow you to systematically drill down to the source of an alarm.

**Table 4-40 Viewing Device Alarms**

Command	Syntax	Description
show alarms		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.

To configure the alarm overload detection, follow these steps:

- Step 1** Choose **Devices > Devices > General Settings > Notification and Tracking > Alarm Settings**. The Alarm Settings page is displayed.
- Step 2** 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 3** 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 4** 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 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.

#### Alarms for Admin Shutdown Interface

When the **Alarms for Admin Shutdown Interface** check box is checked, the interface alarm is shutdown. If there is already an alarm raised when the setting is submitted, unchecking the option and submitting the change does not clear the outstanding alarm. There are two ways to avoid this situation:

1. Clear the outstanding alarm first before disabling this option.
2. Disable this option and reboot. The alarm is cleared during reboot.



- Note** The **Alarms for Admin Shutdown Interface** option should be enabled before any of the above for the alarm to take affect.

To enable the **Alarms for Admin Shutdown Interface** option, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Notification and Tracking > Alarm Settings**. The Alarm Settings page is displayed.
- Step 2** Check the **Alarms for Admin Shutdown Interface** check box to enable this option.
- 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.

---

## 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 4-99.



**Note** Threshold monitoring is performed on each device in the VDS-IS. The protocol engine and NIC bandwidth thresholds are only monitored on the SE. They are not monitored on the SR and CDSM.

---



**Note** The base license limit is set to 200 sessions and 200 Mbps bandwidth.

- The burst count, which indicates the number of days after which a major alarm is raised, is configurable. On the Service Engine, use the **service-router service-monitor threshold burstcnt** command to configure the burst count. The default setting is one (1), which means all of the minor alarms that occur in a single day (24-hour interval) are counted as one single alarm. If the **service-router service-monitor threshold burstcnt** command is set to two, all minor alarms that occur in two days (48-hour interval) are counted as a single alarm.
  - A universal license is similar to a regular license, except it has a higher bandwidth and applies to all protocol engines (except Web Engine). When a universal license is purchased and configured, the alarm data for all protocol engines are cleared. Thereafter, the monitoring of the protocol engines continues as usual for any future alarms.
  - On the Service Engine, use the **service-router service-monitor license-universal enable** command to enable the universal license. The **service-router service-monitor license-universal** command is disabled by default.
- 

To configure workload thresholds, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Notification and Tracking > Service Monitor**. The Service Monitor page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-41](#) for a description of the fields.

**Table 4-41 Service Monitor Fields**

Field	Description
<b>CPU Settings</b>	
Enable	Allows the SR to collect CPU load information from the device.
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 keepalive 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 load allowed. The disk threshold is a disk I/O load threshold setting. It is not used to monitor disk usage, it is calculated using the kernel's diskstats status. This represents how much disk I/O capacity the device is using. It is calculated across all disks on the device. 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.

**Table 4-41 Service Monitor Fields (continued)**

Field	Description
<b>WMT Settings<sup>1</sup></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.
<b>FMS Settings<sup>1</sup></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<sup>1,2</sup></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>NIC Bandwidth Settings<sup>1</sup></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 Percentage</b>	
Threshold	<p>Overall percentage of CDNFS disk failures. The range is from 1 to 100. The default is 75.</p> <p>When the percentage failed disks exceeds this threshold, no further requests are sent to this device. The Disk Failure Threshold is only for the CDNFS disks.</p> <p><b>Note</b> When an alarm is received for a SYSTEM disk, it is immediately marked as a failed disk. It is not checked against the Disk Failure Threshold. The SR continues redirecting to the SE, unless all SYSTEM disks on the SE are marked as failed disks. If disks have both SYSTEM and CDNFS partitions, they are treated as only system disks, which means they are not included in the accounting of the CDNFS disk calculation.</p>

**Table 4-41 Service Monitor Fields (continued)**

Field	Description
<b>Augmentation Alarms</b>	
Enable	Enables augmentation alarms. For more information, see the “ <a href="#">Augmentation Alarms</a> ” section on page 4-86.
Threshold	<p>The augmentation alarms threshold is a percentage, that applies to the CPU, memory, kernel memory, disk, disk fail count, NIC, and protocol engine usages. By default it is set to 80 percent. The threshold value range is 1–100.</p> <p>As an example of an augmentation alarm, if the threshold configured for CPU usage is 80 percent, and the augmentation threshold is set to 80 percent, then the augmentation alarm for CPU usage is raised when the CPU usage crosses 64 percent.</p> <p>If “A” represents the Service Monitor threshold configured, and “B” represents the augmentation threshold configured, then the threshold for raising an augmentation alarm = <math>(A * B) / 100</math> percent. For more information, see the “<a href="#">Augmentation Alarm Example</a>” section on page 4-87.</p>
<b>Transaction Logging</b>	
Enable	Enables Service Monitoring transaction logging. For more information, see the “ <a href="#">Service Monitor Transaction Logs</a> ” section on page 8-90.

1. Protocol engines and NIC bandwidth are only monitored on the SE. They are not monitored on the CDSM and SR.
2. 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.

### 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.

### Augmentation Alarms

Augmentation alarms are soft alarms that send alerts before the threshold is reached. These alarms are applicable to all devices—Service Engines, Service Routers and CDSMs. Augmentation thresholds apply to device and protocol engine parameters.

A different augmentation alarm is supported for each of the device-level thresholds. Based on the device parameters monitored by Service Monitor, the following minor alarms could be raised for device-level thresholds:

- CpuAugThreshold—Service Monitor CPU augmentation alarm.
- MemAugThreshold—Service Monitor memory augmentation alarm.
- KmemAugThreshold—Service Monitor kernel memory augmentation alarm.
- DiskAugThreshold—Service Monitor disk augmentation alarm.
- DiskFailCntAugThreshold—Service Monitor disk failure count augmentation alarm.
- NicAugThreshold—Service Monitor NIC augmentation alarm.

Check the augmentation threshold, device-level threshold, and average load for the above alarm instance. Add more devices if necessary. A useful command is the **show service-router service-monitor** command. The augmentation alarms raised are displayed in the **show alarms detail** command. The alarms are cleared when the load goes below the augmentation threshold.

**Note**

For system disks (disks that contain SYSTEM partitions), only when all system disks are bad is the diskfailure augmentation and threshold alarms raised. The diskfailcnt threshold does not apply to system disks. The threshold only applies to CDNFS disks, which is also the case for the augmentation thresholds. This is because the system disks use RAID1. There is a separate alarm for bad RAID. With the RAID system, if the critical primary disk fails, the other mirrored disk (mirroring only occurs for SYSTEM partitions) seamlessly continues operation. However, if the disk drive that is marked bad is a critical disk drive, the redundancy of the system disks for this device is affected. For more information on disk error handling and threshold recommendations, see the “[Enabling Disk Error Handling](#)” section on page 4-61.

As the **show disk details** command output reports, if disks have both SYSTEM and CDNFS partitions, they are treated as only system disks, which means they are not included in the accounting of the CDNFS disk calculation.

**Note**

The NIC augmentation alarm is only applicable if the device is an SE.

Different augmentation alarms are supported for each of the protocol engines, which only apply if the device is an SE. The following minor alarms could be raised for protocol-engine thresholds:

- rtspaugmentexceeded— RTSP gateway TPS has reached augmentation threshold limits
- aug\_memory\_exceeded—Web Engine augmentation memory threshold exceeded
- aug\_session\_exceeded—Web Engine has reached augmentation threshold for concurrent session
- wmtaugmentexceeded—Windows Media Streaming has reached augmentation threshold limits
- msaugmentexceeded—Movie Streamer has reached augmentation threshold limits
- FmsAugThreshold—Flash Media Streaming has reached augmentation threshold limits
- WebCalLookupAugThreshold—Web Engine has reached augmentation threshold for storage lookup
- WebCalDiskWriteAugThreshold—Web Engine has reached augmentation threshold for storage disk write

#### Augmentation Alarm Example

Maximum concurrent connections have a default value of 200 and maximum bandwidth has a default value of 200 Mbps. The augmentation alarm is enabled through the Service Monitor and the augmentation threshold is configured at 80 percent (default). The default service threshold for Flash Media Streaming is 90 percent.

In this case, the augmentation alarm is raised for Flash Media Streaming when  $0.8 * 0.9 * 200 = 144$  connections or 144 Mbps of bandwidth is exceeded. The Service Router still redirects requests to this Service Engine. The alarm is cleared when the traffic falls below either of the thresholds; that is, 144 connections or 144 Mbps in this example.

#### Enabling System Monitor Settings

The System Monitor page is where you configure the uninterruptible sleep process check for the device. To configure system monitor settings, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Notification and Tracking > System Monitor**. The System Monitor Settings for Service Engine page is displayed.

- Step 2** To enable uninterruptible sleep process check, check the **Enable** checkbox in the Uninterruptible Sleep Process Check pane.
- 

## Configuring SNMP

The Cisco VDS-IS 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 inter-operable 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 as follows:
  - 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 4-42](#) identifies what the combinations of security models and levels mean.

**Table 4-42      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 Content 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.

To configure the SNMP settings, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Notification and Tracking > SNMP > General Settings**. The SNMP General Settings page is displayed.
- Step 2** Enable the settings as appropriate. See [Table 4-43](#) for a description of the fields.

**Table 4-43      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.

**Table 4-43** SNMP General Settings Fields (continued)

Field	Description
Config	Enables CiscoConfigManEvent error traps.
<b>Miscellaneous Settings</b>	
Notify Inform	Enables the SNMP notify inform request.

**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.

**Step 4** From the left-panel menu, choose **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 5** 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.



**Note** Each community is associated with a group. Each group has a view and users are assigned to a group. If the group does not have a view associated with it, then users associated that group cannot access any MIB entry.

**Step 6** Enter the settings as appropriate. See [Table 4-44](#) for a description of the fields.

**Table 4-44** 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 7** 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 8** From the left-panel menu, choose **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 9** 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 10** Enter the settings as appropriate. See [Table 4-45](#) for a description of the fields.

**Table 4-45** *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 of 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>• noAuthNoPriv—Authenticates a packet by a string match of the username.</li> <li>• AuthNoPriv—Authenticates a packet by using either the HMAC MD5 or SHA algorithms.</li> <li>• AuthPriv—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>

**Table 4-45** SNMP Group Fields (continued)

Field	Description
Write View	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.  A write view defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.
Notify View	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.  A notify view defines the list of notifications that can be sent to each user in the group.

**Step 11** 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 12** From the left-panel menu, choose **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 13** 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 14** Enter the settings as appropriate. See [Table 4-46](#) for a description of the fields.

**Table 4-46** SNMP User Fields

Field	Description
Name	String representing the name of the user (256 characters maximum) who can access the device.  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>

**Table 4-46** SNMP User Fields (continued)

Field	Description
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. 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 15** 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 16** 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 17** 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 18** Enter the settings as appropriate. See [Table 4-47](#) for a description of the fields.

**Table 4-47** 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> <b>Note</b> When configuring an SNMP View with Excluded, the specified MIB that is excluded is not accessible for the community associated with the group that has that view.

**Step 19** 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 20** From the left-panel menu, choose **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 21** 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 22** Enter the settings as appropriate. See [Table 4-48](#) for a description of the fields.

**Table 4-48      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.
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 23** 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 24** From the left-panel menu, choose **Asset Tag**. The SNMP Asset Tag page is displayed.

**Step 25** 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 26** From the left-panel menu, choose **Contact**. The SNMP Contact page is displayed.

**Step 27** In the **Contact** field, enter a name of the contact person for this device.

**Step 28** In the **Location** field, enter a location of the contact person for this device.

**Step 29** 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)
- BGP-4-MIB (RFC-4274)
- UCD-SNMP-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-CONFIG-MAN-MIB (Revision 9511280000Z)
- CISCO-SERVICE-ENGINE-MIB (supports streaming media-related MIB objects)

ENTITY-MIB, MIB-II, HOST-RESOURCES-MIB, BGP-4-MIB, and UCD-SNMP-MIB are public-available MIBs.

To download a copy of the CISCO-SERVICE-ENGINE-MIB, follow these steps:

---

**Step 1** Choose **System > CDS-IS Files > SNMP MIB**. The CISCO\_SERVICE-ENGINE-MIB.my is listed.

**Step 2** Click one of the following links:

- **CISCO\_SERVICE-ENGINE-MIB.my**
- **CISCO\_CDS\_SERVICE\_ROUTING\_MIB.my**

Your browser program displays a dialog box asking if you want to open or save the file.

**Step 3** Choose the appropriate option; either open or save the file.

---

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.

The CISCO\_CDS\_SERVICE\_ROUTING\_MIB.my provides some object identifiers (OIDs) for Service Router statistics. All the OIDs in the MIB are only for querying purposes; no traps have been added to this MIB. The Service Router MIB provides two groups, cdssrStatsGroup and cdssrServiceMonitorGroup, which contain OIDs for the statistics from the **show statistics service-router summary/dns/history/se/content-origin** command and the **show service-router service-monitor** command.

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.

## 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 /local/local1/syslog.txt.

To enable system logging, follow these steps:

- Step 1** Choose **Devices > Devices > General Settings > Notification and Tracking > System Logs**. The System Log Settings page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-49](#) for a description of the fields.

**Table 4-49 System Logs Settings Fields**

Field	Description
<b>System Logs</b>	
Enable	Enables system logs.
Facility	Facility where the system log is sent.
<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: Emergency—System is unusable. Alert—Immediate action needed. Critical—Critical condition. Error—Error conditions. Warning—Warning conditions. Notice—Normal but significant conditions. Information—Informational messages. 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 /local/local1/syslog.txt.

**Table 4-49 System Logs Settings Fields (continued)**

Field	Description
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 3** 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.

## Configuring 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.

### Enabling the Kernel Debugger

To enable the kernel debugger, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Troubleshooting > Kernel Debugger**. The Kernel Debugger page appears.
- Step 2** 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 8-13.

## Configuring Service Router Settings

The keepalive interval is used by the SE to send keepalive messages to the SR. If the SE is configured with more than one streaming interface (multi-port support), the keepalives are sent for each streaming interface.

To configure the keepalive interval the SE uses for messages to this SR, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Service Routing Settings**. The Service Routing Settings page is displayed.
- Step 2** 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 seconds.
- Step 3** In the **Snapshot Counter Report Interval** field, enter the report interval for the wholesale snapshot counter report. The range is from 5 to 180. The default is 10 seconds.
- 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 Cache Router Settings

To configure the liveness interval the SE uses for messages to this SR, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Cache Router**. The Cache Router page is displayed.
- Step 2** From the **Select a Device Group** drop-box, choose the device group.
- Step 3** In the **Liveness Query timeout** field, enter the number of milli seconds the messages from the SR should be kept alive on this SE. The range is from 1 to 1000. The default is 200 seconds.
- 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 Memory Limitation Settings

To configure the memory limitation settings for an SE, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Memory Limitation**. The Memory Limitation page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-50](#) for a description of the fields.

**Table 4-50      Memory Limitation Settings Fields**

Field	Description
contentmgr	Memory size for Content Manager. If the physical memory size is greater or equal to 32GB, the default value is 16GB, otherwise the default value is 6GB.
fms-server	Memory size for Flash Media Server. If the physical memory size is greater or equal to 48GB, the default value is 8GB. If the physical memory size is between 48GB and 32GB, the default value is 6GB, otherwise the default value is 4GB.
movie-streamer	Memory size for Movie Streamer. The default value is 4GB.
webengine	Memory size for Web Engine. If the physical memory size is greater or equal to 32GB, the default value is 12GB. If the physical memory size is between 32GB and 16GB, the default value is 8GB, otherwise the default value is 4GB.

- 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 Service Router

Configuring a Service Router (SR) consists of the following procedures:

- [Activating a Service Router, page 4-100](#)
- [Configuring Routing Settings, page 4-104](#)
- [Configuring Application Control, page 4-122](#)
- [Configuring Load Monitoring, page 4-122](#)
- [Configuring Last-Resort Routing, page 4-124](#)
- [Configuring Domain Subscription, page 4-128](#)
- [Configuring Memory Limitation Settings, page 4-128](#)
- [Configuring Transaction Logs for the Service Router, page 4-129](#)

For information on configuring the general settings, except last-resort routing and transaction logging, see the “General Settings” section on [page 4-46](#).

## 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, follow these steps:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the SR that 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 4-51](#) for a description of the fields.

**Table 4-51      Service Router Activation Fields**

Field	Description
Name	Name of the device.
Location	The Location drop-down list lists all of the location configured for the VDS-IS.
Activate	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.  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 VDS-IS Network Device Registration Information</a> ” section on page 9-25

**Table 4-51      Service Router Activation Fields (continued)**

Field	Description
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, see the “<a href="#">Configuring Port Channel</a>” section on page I-6 for more information.</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 the Software</a>” section on page 9-6.</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>SR &amp; Proximity Engine</b> if you want to enable the Proximity Engine; otherwise, choose <b>Service Router only</b>. For more information, see the “<a href="#">Configuring the Proximity Server Settings</a>” section on page 4-111.</p>
Coverage Zone File	<p>To have a local Coverage Zone file overwrite the VDS-IS 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>,” page 6-12 for information about creating and registering a Coverage Zone file. Otherwise, choose <b>None</b>.</p>

**Table 4-51 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</a>” section on page 4-69 and the “<a href="#">Configuring Port Channel</a>” section on page I-6.</p>
Management Communication Port	Port number to enable communication between the CDSM and the SR.
Monitor SE Keepalive Message on	<p>From the <b>Monitor SE Keepalive Message on</b> drop-down list, choose the IP address for the device.</p> <p>This feature allows an SR to listen to private IP addresses on which it receives KAL/SCR from SEs. The private IP addresses can be accessed by the devices within the VDS-IS network. Therefore prevents attacks from the Internet for this UDP port 2323.</p> <p>For more information to enable or disable this feature, see the <a href="#">Configuring the Monitor SE Keepalive Messages, page 4-102</a></p>
Comments	Information about the settings.

 **Note** To make sure that the SR is binding to the primary interface (or management IP address if configured) as the source IP address when sending management traffic to the CDSM, create a static route from the SR to the CDSM. To configure a static IPv4 route from the SR, see the “[Configuring Static Routes](#)” section on page 4-79. To configure a static IPv6 route from the SR, see the “[Configuring Static IPv6 Routes](#)” section on page 4-80. Alternatively, you can use the **ip route** command and **IPv6 route** command on the VDS-IS device.

### Configuring the Monitor SE Keepalive Messages

To enable or disable the **Monitor SE Keepalive Message on** feature, follow these steps:

 **Note** While enabling or disabling this option, you must offload the SR to make sure that the KAL/SCR messages are not lost.

The procedure must be followed when you want to downgrade a CDN from a version with the feature enabled, to an old version that does not support this feature.

### Prerequisites

To enable this feature, the following conditions should be satisfied:

- The administrator must have already setup the VDS-IS network with private IPs for all devices. The administrator must make sure that SEs and SRs are able to communicate with each other through the private IP addresses.
- The administrator must make sure that the UDP port 2323 is not accessible by unauthorized entities outside the VDS-IS network.
- The administrator must make sure that the software versions for all the devices including SEs, SRs, and CDSMs are supporting this feature.



**Note** There may be KAL/SCR message losses if a device is not on a version that supports this feature.

- While enabling or disabling **Monitor SE Keepalive Message on** feature, the feature is enabled or disabled for each SR one by one.

To offload the SR, follow these steps:

**Step 1** Wait for 120 seconds, then from the **Devices > Device Activation > Monitor SE Keepalive Message on** drop-down list:

- Select the right IP, to enable the feature.
- Select **All**, to disable the feature.

**Step 2** Wait for 60 seconds, then check to see if there is an **SeKeepalive** alarm for any SE on this SR; if there is no SeKeepalive alarm, go to the [Step 3](#).

- If there is any **SeKeepalive** alarm on the SR, wait for another **System.datafeed.pollRate** seconds (300 seconds by default)
- If any **SeKeepalive** alarm persists for an SE, there is a configuration issue with the SE, try to resolve it.
- Repeat the previous steps until no **SeKeepalive** alarm exists on the SR.
- Un-offload the SR to bring it back online

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

## Configuring Routing Settings

The Routing Settings pages provide settings for the Request Routing Engine and the Proximity Engine. Configuring the Service Router engines consists of the following procedures:

- [Configuring Request Routing Settings, page 4-104](#)
- [Configuring IP-based Redirection, page 4-109](#)
- [Configuring DNS-based Redirection, page 4-109](#)
- [Configuring Redirect Burst Control, page 4-110](#)
- [Configuring Cross-Domain Policy, page 4-110](#)
- [Configuring the Proximity Server Settings, page 4-111](#)

The Service Router has two engines, the Request Routing Engine and the Proximity Engine.

The Proximity Engine contains the functionality of the Proximity Servers used for proximity-based routing. For more information, see the “Service Router” section on page 1-34.

## Configuring Request Routing Settings

To configure the Request Routing Settings, follow these steps:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Devices &gt; Devices &gt; Routing Settings &gt; Request Routing Settings &gt; General Settings</b> . The Request Routing Settings page is displayed. |
| <b>Step 2</b> | Enter the settings as appropriate. See <a href="#">Table 4-52</a> for a description of the fields.   |

**Table 4-52 Request Routing Settings—General Settings Fields**

Field	Description
Enable Location Based Routing	When location-based routing is enabled, the Service Router first looks up the client’s IP address in the Coverage Zone file. If there is no subnet in the Coverage Zone file that matches the client’s IP address, the client’s geographical location is compared to the geographical location of the Service Engines listed in the Coverage Zone file, and the closest and least-loaded Service Engine is selected. Geographically locating a client is used when users roam outside of their home networks.
Location Cache Timeout	Enter the timeout interval (in seconds) that a response from the Geo-Location server is stored in the SR cache.  The SR caches information from the Geo-Location server during the first request so that further requests can be served from cache instead of contacting the Geo-Location server.  The default is 691200. The range is 1 to 864000.

**Table 4-52 Request Routing Settings—General Settings Fields (continued)**

Field	Description
Type	<p>Server type.</p> <ul style="list-style-type: none"> <li>• Quova—if <b>quova</b> is selected from the <b>Type</b> drop-down list:           <ul style="list-style-type: none"> <li>– In the <b>Primary Address</b> and associated <b>Port</b> fields, enter the IPv4 address and port number of the primary Geo-Location Server.</li> <li>– In the <b>Secondary Address</b> and associated <b>Port</b> fields, enter the IPv4 address and port number of the secondary Geo-Location Server.</li> </ul> </li> <li>• Quova GDS (Version 7.1.5)—If <b>quova-restful-gds</b> is selected from the Type drop-down list:           <ul style="list-style-type: none"> <li>– In the <b>Primary Address</b> and associated <b>Port, Service Name, Retry</b> and <b>Timeout</b> fields, enter the IPv6 or IPv4 address, port number, Service name, Retry and Timeout of the primary Geo-Location Server.</li> <li>– In the <b>Secondary Address</b> and associated <b>Port, Service Name, Retry</b> and <b>Timeout</b> fields, enter the IPv6 or IPv4 address, port number, Service name, Retry and Timeout of the secondary Geo-Location Server.</li> </ul> </li> <li>• Quova Hosted—if <b>quova-restful-hosted</b> is selected from the <b>Type</b> drop-down list:           <ul style="list-style-type: none"> <li>– In the <b>API Key</b> field, enter the API key of the Geo-Location Server.</li> <li>– In the <b>Shared Secret Key</b> field, enter the shared secret key of the Geo-Location Server.</li> <li>– In the <b>Primary Address</b> and associated <b>Port, Service Name, Retry</b> and <b>Timeout</b> fields, enter the IPv6 or IPv4 address, port number, Service name, Retry and Timeout of the primary Geo-Location Server.</li> <li>– In the <b>Secondary Address</b> and associated <b>Port, Service Name, Retry</b> and <b>Timeout</b> fields, enter the IPv6 or IPv4 address, port number, Service name, Retry and Timeout of the secondary Geo-Location Server.</li> </ul> </li> <li>• MaxMind Hosted—if the <b>maxmind-restful-hosted</b> is selected from the <b>Type</b> drop-down list:           <ul style="list-style-type: none"> <li>– From the <b>Protocol</b> drop-down list, choose <b>Http</b> or <b>Https</b>.</li> <li>– In the <b>Service</b> field, enter the service name. The service name can be a, b, f, or e.</li> <li>– In the <b>License Key</b> field, enter the key that is used by the Geo-Location server to verify a request.</li> <li>– In the <b>Primary Address</b> and associated <b>Port, Retry</b> and <b>Timeout</b> fields, enter the IPv6 or IPv4 address, port number, Retry and Timeout of the primary Geo-Location Server.</li> <li>– In the <b>Secondary Address</b> and associated <b>Port, Retry</b> and <b>Timeout</b> fields, enter the IPv6 or IPv4 address, port number, Retry and Timeout of the secondary Geo-Location Server.</li> </ul> </li> </ul>

**Note**

The Maxmind server service supported is GeoIP Legacy web services  
<http://dev.maxmind.com/geoip/legacy/web-services/>.

**Table 4-52 Request Routing Settings—General Settings Fields (continued)**

Field	Description
Primary Geo-Location Server IP address and Port	The IP address and port number of the primary Geo-Location Server for location-based routing. For more information, see the “Geo-Location Servers” section on page 4-107.
Secondary Geo-Location Server IP address and Port	The IP address and port number of the secondary Geo-Location Server.
Enable Content Based Routing	<p>When enabled, the SR redirects requests based on the URI. Requests for the same URI are redirected to the same SE, provided the SE’s thresholds have not been exceeded. This optimizes disk usage in the VDS-IS by storing only one copy of the content on one SE, instead of multiple copies on several SEs. For more information about content-based routing, see the “Content-Based Routing” section on page 1-44.</p> <p><b>Note</b> Content-based routing does not work with clients sending signed URL requests. The hashing algorithm for content-based routing considers the whole signed Url, so a signed URL request for the same content may be redirected to a different SE.</p>
Number of Redundant Copies	Number of copies of a content to keep among SEs in a Delivery Service. The range is from 1 to 4. The default is 1. If redundancy is configured with more than one copy, multiple Service Engines are picked for a request with the same URI hash.
Enable Proximity Based Routing	<p>When enabled, the SR contacts the Proximity Server with the client IP address and a list of SEs. The Proximity Server returns a list of SEs ordered by distance or metric, and provides a client subnet mask. The SR caches this information for this client. The SR redirects the client request to the SE selected, which is based on load, availability, and Delivery Service subscription.</p> <p>To configure a standalone Proximity Engine, see the <i>Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference</i>.</p> <p>To configure a collocated Proximity Engine, see the “Configuring the Proximity Server Settings” section on page 4-111.</p> <p>For more information, see the “Proximity-Based Routing” section on page 1-41.</p>

**Table 4-52 Request Routing Settings—General Settings Fields (continued)**

Field	Description
Proximity Cache Timeout	The maximum number of seconds the proximity response from the Proximity Server is valid for a client subnet. After the Proximity Cache Timeout period has elapsed, any new request from the same client subnet causes the SR to query the Proximity server for a new proximity response. The proximity range is from 1 to 86400. The default is 1800.  Proximity ratings for overlapping subnets are not cached.
Proximity Server Host [1-8]	The IP address of the Proximity Server. If you are using the collocated Proximity Engine as one of the Proximity Servers, enter 127.0.0.1 as the IP address.
Password	The selection of the Proximity Server is based on the lowest IP address. If there is only one Proximity Server, the SR uses that server. If another Proximity Server is configured with an IP address lower than the first one, the SR sends a request to the newly configured Proximity Server, and if it responds, the SR uses the new Proximity Server with the lower IP address.  Password of the Proximity Server.  For more information on configuring the Proximity Engine, see the “ <a href="#">Configuring the Proximity Server Settings</a> ” section on page 4-111.

**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.

## Geo-Location Servers

The Geo-Location servers work with the following VDS-IS features:

- Location-based routing
- Authorization Service

For location-based routing, the Geo-Location servers identifies the latitude and longitude of a client based on the IP address of the client. The Request Routing Engine compares the latitude and longitude of each Service Engine, which is defined in the Coverage Zone file, with the latitude and longitude of the client to assign a Service Engine that is geographically closest to the client. For more information on location-based routing, see the “[Location-Based Routing](#)” section on page 1-41 and Appendix C, “[Creating Coverage Zone Files](#).”

For Authorization Service, the Geo-Location servers identify the city, state, country, Netspeed, connection\_type, line\_speed, asn, carrier, and anonymizer\_status of the client based on the IP address of the client. The Authorization Service on the Service Engine compares the city, state, and country of the client with city, state, and country defined in the Authorization Service file. If a match is found, the client is either allowed or denied based on what is specified in the Authorization Service file. For more information about configuring the Authorization Service, see the “[Configuring the Authorization Service](#)” section on page 4-28.



**Note** Starting with Release 3.3, in addition to the city, state, and country, the Geo-Location servers will also identify Netspeed, connection\_type, line\_speed, asn, carrier, and anonymizer\_status of the client based on the IP address of the client.

### Caching Geo-Location Server Information

The SR or SE caches the Geo-Location information returned from the Geo-Location servers and the device (SE or SR) queries their own cache first before contacting the Geo-Location servers. If the IP address of the client is found in the cache on the device, the lookup is performed using that information and the Geo-Location servers are not contacted.

For location-based routing, the SR caches up to 10,000 IP addresses. The IP addresses are discrete, which means that they do not describe subnets. By default, the cached information expires after 8 days (691,200 seconds). The time interval that the cache expires is configurable by setting the **Location Cache Timeout** field. If the cache is full, the entries are replaced according to the least recently used (LRU) mechanism.

For Authorization Service, the SE caches information on the country of 10,000 clients. The cached information expires after 8 days. If the cache is full, the entries are replaced according to the LRU mechanism.



**Note** Currently, there is no command to clear the Geo-location cache on the device.

Starting with Release 3.3, if the Geo Server type is changed, for example, Quova GDS to Quova Hosted, MaxMind Hosted service b to MaxMind Hosted service e, the cache will be cleared.

### Redundant Geo-Location Servers

The VDS-IS offers the ability to configure primary and secondary Geo-Location servers. In the event that the primary server is unreachable, the secondary Geo-Location server is contacted. The secondary Geo-Location server is then used unless it becomes unreachable, in which case the primary Geo-Location server is contacted. The Geo-Location server configuration determines the time to wait before failing over to the other server. The default is 245 milliseconds.

For the location-based routing feature, and the Authorization Service feature, the cached client information on the VDS-IS device is checked first before querying the Geo-Location servers.

For location-based routing, if both primary and secondary Geo-Location servers are down, the VDS-IS uses the default route configured through the zero-IP based configuration in the Coverage Zone file. For more information, see the “[Zero-IP Based Configuration](#)” section on page C-2.

For Authorization Service, if both the primary and secondary Geo-Location servers are down, a request denied message is returned to the client. The type of message that is returned depends on the protocol engine (for example, the Flash Media Streaming engine sends “Denied by auth server”). However, the client receives the same denied message from the protocol engine whether the client is denied based on the Authorization Service configuration, or based on the Geo-Location servers being down and the client information not being available in the SE cache.

### Communicating with Geo-Location Servers

VDS-IS supports the following Geo servers:

- quova
- quova-restful-gds

- quova-restful-hosted
- maxmind-restful-hosted

The Geo-location information of a client IP address is obtained from an external server. The VDS-IS communicates with the quova servers by using a proprietary version of TCP. RESTful API is used to communicate with quova-restful-gds servers, quova-restful-hosted servers, and maxmind-restful-hosted servers.

## Configuring IP-based Redirection

IP-based redirection uses IP addresses to route client requests to the SR and on to the SE. For more information, see the “[IP-Based Redirection](#)” section on page 1-37.



**Note** The Web Engine does not support IP-based redirection.

To enable IP-based redirection, follow these steps:

- 
- Step 1** Choose **Devices > Devices > Routing Settings > Request Routing Settings > IP-Based Redirection**. The IP-Based Redirection page is displayed.
- Step 2** Check the **Enable IP-based Redirection** 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.
- 

## Configuring DNS-based Redirection

DNS-based redirection uses the status of the Web Engine to route the client requests to the SR.

To enable DNS-based redirection, follow these steps:

- 
- Step 1** Choose **Devices > Devices > Routing Settings > Request Routing Settings > DNS Based Redirection**. The DNS Based Redirection page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-53](#) for a description of the fields.

**Table 4-53 DNS Based Redirection Fields**

Enable Redirect Based on WE Status	Check the <b>Enable Redirect Based on WE Status</b> check box to enable Redirection based on the Web Engine status. The <b>Enable Redirect Based on WE Status</b> is disabled by default.
Enable for All Domains	<p>Check the <b>Enable for All Domains</b> check box to enable Redirection for all domains. The <b>Enable for All Domains</b> is disabled by default.</p> <p><b>Note</b> A domain list will be maintained if <b>Enable for All Domains</b> is not selected.</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 Redirect Burst Control

The SR learns about the state of the SEs through the keepalive messages between the SEs and the SR. The keepalive messages occur every two seconds. If a burst of client requests occurs between two keepalive messages, the SR may not know about the current state of the SE, and might route a request to an already overloaded SE. This scenario can happen during mixed traffic, because each protocol engine has different memory and CPU requirements.

The Redirect Burst Control page allows you to configure how many requests (transactions per second [TPS]) the SR should redirect to an SE during a burst.

To configure the redirect burst control, follow these steps:

**Step 1** Choose **Devices > Devices > Routing Settings > Request Routing Settings > Redirect Burst Control**. The Redirect Burst Control page is displayed.

**Step 2** Check the **Enable Redirect Burst Control** check box. The Redirect Burst Control is disabled by default.

**Step 3** In the Rate field, enter the maximum TPS the SR can send to an SE. The default is 100000. The range is from 1 to 100000.

**Step 4** 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 Cross-Domain Policy

The Access Policy page allows you to enable the Cross-Domain Policy feature on the SR. For more information, see the “[Cross-Domain Policy](#)” section on page 1-46.

To enable the cross-domain policy, follow these steps:

**Step 1** Choose **Devices > Devices > Routing Settings > Request Routing Settings > Access Policy**. The Access Policy page is displayed.

**Step 2** Check the **Enable Access Policy** 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.

---

## Configuring the Proximity Server Settings

The Proximity Server Settings are available when you choose the **SR & Proximity Engine** as the **Work Type** in the Device Activation page for the SR. See the “Activating a Service Router” section on page 4-100 for more information. The Proximity Server Settings pages are only for a Proximity Engine that is collocated with the SR. To configure a standalone Proximity Engine, see the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference*.

To include the Proximity Engine on the SR as one of the Proximity Servers, you must enable proximity-based routing and add 127.0.0.1 as one of the Proximity Servers. See the “Configuring Request Routing Settings” section on page 4-104 for more information.

**Note**

The Proximity Engine is only supported on the CDE205 platform.

For more information on the Proximity Engine, see the “Proximity Engine” section on page 1-47.

The Proximity Server Settings for the Proximity Engine consists of the following pages:

- General Settings—Enables the BGP proximity algorithms
- IS-IS—Configures IS-IS adjacencies
- OSPF—Configures the OSPF adjacencies
- BGP—Configures the location community for the BGP community-based proximity
- SRP—Configures Service Routing Protocol (SRP)

IGP and BGP protocol peering with the network routers are the basic building blocks for the proximity calculation. The peering with the routers is to learn the network topology and compute the best path for each prefix. Prefixes are deposited to the routing information base (RIB).

**Note**

Although the Proximity Engine participates in both IGP and BGP with the routers, the routes that the Proximity Engine learns are purely for proximity computation only. Proximity Engine is not a router.

For the proximity function to work, at least one of the following is required:

- Enabled link-state protocol, such as OSPF or IS-IS for IGP proximity, which is required if the Proximity Engine is going to peer with IGP routers.
- Enabled policy routing protocol, such as BGP for best-path proximity and location-community proximity, which is required if the Proximity Engine is going to peer with BGP routers.

**Note**

All BGP routes must resolve to IGP next hops or directly connected routes.

**Note**

Only one IGP (IS-IS or OSPF) is supported for the Proximity Engine.

## Enabling the BGP Proximity Algorithms

See the “BGP Proximity Algorithms” section on page 1-50 for more information.

To enable the BGP community-based proximity, follow these steps:

**Step 1** Choose **Devices > Devices > Routing Settings > Proximity Server Settings > General Settings**. The Proximity Routing General Settings page is displayed.

**Step 2** To enable the BGP best-path proximity, check the **Enable proximity algorithm BGP best-path** check box.



**Note** The BGP best-path proximity algorithm requires the configuration of the BGP proximity settings. See the “[Configuring the BGP Community-based Proximity Settings](#)” section on [page 4-118](#).

**Step 3** To enable the BGP community-based proximity, check the **Enable proximity algorithm BGP location-community** check box, and from the **Match mode** drop-down list, choose either **Normal** or **Strict**.

The **Strict** option instructs the Proximity Engine to return **UINT-MAX** as the proximity rating for PTAs that are not associated with the PSA by way of any location-community attribute. This setting is global and applies to all proximity requests. If PSA is BGP and has no community attributes, then all PTAs get **UINT\_MAX** rating. If the PSA is IGP, then this setting does not apply and other proximity algorithms, BGP best-path and IGP metric, are used to rate the PTAs in the proximity request.

The **Normal** option retains the normal functioning of the BGP proximity algorithm.

**Step 4** To enable the BGP redirect proximity, check the **Enable proximity algorithm BGP redirect** check box.



**Note** The redirect proximity algorithm requires the configuration of the BGP and the SRP proximity settings. See the “[Configuring the BGP Community-based Proximity Settings](#)” section on [page 4-118](#) and the “[Configuring SRP](#)” section on [page 4-121](#) for more information.

**Step 5** Click **Submit**.

To remove the settings, click the **Delete** icon.

To restore the default settings, click the **default settings** icon.

## Configuring the IS-IS Adjacencies

The Proximity IS-IS page allows the Proximity Engine to establish an adjacency with its directly connected neighbor and to receive the whole LSDB content. Protocol parameters, such as IS-type and IS network entity title (NET), vary according to network topology and deployment.

IS-IS is a link-state routing protocol for IGP. Its protocol stack runs directly on Layer 2. The main characteristic of the link-state protocols is that every node in the network contains an exact view of the routing topology. It has faster convergence than vector distance protocols. Each node in the network generates a link state packet (LSP) to describe its neighbors. The LSP is flooded throughout the network to every node. Reliability of the flooding is obtained by Complete Sequence Number Packet (CSNP) which is sent by the Designator Router (DR) periodically in the LAN. CSNP describes all of the LSPs that the DR contains. The receiver of the CSNP can compare what it has against what is listed in the CSNP and requests the missing LSPs from the DR. Each node uses Dijkstra's algorithm (shortest path first [SPF]) to compute the routes from the LSPs. Routes are then added into the routing information base (RIB).



**Note** Only one IGP (IS-IS or OSPF) is supported for the Proximity Engine.

To configure the IS-IS adjacencies, follow these steps:

- 
- Step 1** Choose **Devices > Devices > Routing Settings > Proximity Server Settings > IS-IS > General Settings**. The Proximity IS-IS page is displayed.
  - Step 2** To enable ISIS adjacencies, check the **Enable** check box and click **Submit**. The Create new Proximity IS-IS interface icon is displayed.
  - Step 3** Enter the settings as appropriate. See [Table 4-54](#) for a description of the fields.

**Table 4-54 Proximity IS-IS Fields**

Field	Description
Network Entity	<p>Enter the Network Entity (network entity title [NET]) for a Connectionless Network Service (CLNS). Under most circumstances, one and only one NET must be configured. A NET is a network service access point (NSAP) where the last byte is always zero and the length can be 8 to 20 bytes. The last byte is always the n-selector and must be zero.</p> <p>The six bytes directly in front of the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2). All bytes in front of the system ID are the area ID. The area ID must match the area ID of the IS-IS router that the Proximity Engine is peering with.</p> <p>A NET must be configured to define the system ID and area ID.</p>
Enable log-adjacency-changes	Check the <b>Enable log-adjacency-changes</b> check box to enable logging of changes to adjacency. When enabled, syslog messages are sent whenever an IS-IS neighbor goes up or down.
LSP MTU	Set the maximum transmission unit (MTU) size, in bytes, for link state packets (LSPs). The LSP MTU size describes the amount of information that can be recorded in a single LSP. The LSP MTU range is from 128 to 4352. If the LSP MTU is not configured, the default is used. The default is 1492.

**Table 4-54 Proximity IS-IS Fields (continued)**

Field	Description
IS-Type	<p>From the <b>IS-Type</b> drop-down list, choose one of the following routing algorithms:</p> <ul style="list-style-type: none"> <li>• <b>level-1</b>—Level 1 is intra-area. The Proximity Engine learns only about destinations inside its area.</li> <li>• <b>level-1-2</b>—The Proximity Engine runs both Level 1 and Level two routing algorithms.</li> </ul> <p>For Level 1, it has one link state packet database (LSDB) for destinations inside the area (Level 1) and runs a shortest path first (SPF) calculation to discover the area topology.</p> <p>For Level 2, it also has another LSDB with link-state packets (LSPs) of all other backbone (Level 2) routers, and runs another SPF calculation to discover the topology of the backbone, and the existence of all other areas.</p> <ul style="list-style-type: none"> <li>• <b>level-2</b>—The Proximity Engine communicates with Level 2 (inter-area) routers only. The Proximity Engine is part of the backbone and does not communicate with Level 1-only routers in its own area.</li> </ul> <p>The default is <b>level-1-2</b>.</p>
Authentication Type [Level-1 or Level-2]	<p>From the <b>Authentication Type Level-1</b> drop-down list or the <b>Authentication Type Level-2</b> drop-down list, choose one of the following authentication types for the corresponding level:</p> <ul style="list-style-type: none"> <li>• <b>None</b>—Do not use MD-5 authentication</li> <li>• <b>cleartext</b>—Do not encrypt the key</li> <li>• <b>md5</b>—Encrypt the key</li> </ul>
Enable Authentication Check [Level-1 or Level-2]	<p>To enable authentication check for Level 1, check the <b>Enable Authentication Check Level-1</b> check box. To enable authentication check for Level 2, check the <b>Enable Authentication Check Level-2</b> check box.</p> <p>When enabled, packets that do not have the proper authentication are discarded. When disabled, IS-IS adds authentication to the outgoing packets, but does not check authentication on incoming packets, which allows for enabling authentication without disrupting the network operation.</p>
Authentication KeyChain [Level 1 or Level-2]	<p>Specify the key chain to be used for the authentication for corresponding level. The key chain can be up to 64 alphanumeric characters.</p>

- Step 4** Click **Submit**. The **Create new Proximity IS-IS Interface** icon displays. To delete the IS-IS configuration, click the **Delete** icon.
- Step 5** To configure the proximity IS-IS interface, click the **Create new Proximity IS-IS Interface** icon. The Proximity IS-IS Interface page is displayed.
- Step 6** From the **Name** drop-down list, choose an interface to configure for IS-IS. The number of available interfaces depends on the CDE.
- Step 7** Enter the settings as appropriate. See [Table 4-55](#) for a description of the fields.

**Table 4-55 Proximity IS-IS Interface Fields**

Field	Description
Enable IP IS-IS router	Check the <b>Enable IP IS-IS router</b> check box to enable IS-IS routing protocol on this interface.
IS-IS Priority for level-1	Enter the priority of this interface for IS-IS Level 1(intra-area) priority. The higher the priority value, the more likely a router becomes the designated router (DR) in the Level 1 area; therefore, because the Proximity Engine is not a router, make sure the priority level is such that it will not interfere with the election of the DR. The <b>IS-IS Priority for level-1</b> range is from 0 to 127. The default is 64.
IS-IS Priority for level-2	Enter the priority of this interface for IS-IS Level 2 (inter-area) priority. The higher the priority value, the more likely a router becomes the designated router (DR) in the Level 2 area; therefore, because the Proximity Engine is not a router, make sure the priority level is such that it will not interfere with the election of the DR. The <b>IS-IS Priority for level-2</b> range is from 0 to 127. The default is 64.
IS-IS Circuit Type	From the <b>IS-IS Circuit Type</b> drop-down list, choose one of the following adjacency levels: <ul style="list-style-type: none"> <li>• <b>level-1</b>—For Level 1 adjacency</li> <li>• <b>level-1-2</b>—For Level 1 and Level 2 adjacency</li> <li>• <b>level-2</b>—For Level 2 adjacency</li> </ul> The default is <b>level-1-2</b> .
IS-IS Authentication Type [Level-1 or Level-2]	From the <b>Authentication Type Level-1</b> drop-down list or the <b>Authentication Type Level-2</b> drop-down list, choose one of the following authentication types for the corresponding level: <ul style="list-style-type: none"> <li>• <b>None</b>—Do not use MD-5 authentication</li> <li>• <b>cleartext</b>—Do not encrypt the key</li> <li>• <b>md5</b>—Encrypt the key</li> </ul>
Enable IS-IS Authentication Check [Level-1 or Level-2]	To enable authentication check for Level 1, check the <b>Enable Authentication Check Level-1</b> check box. To enable authentication check for Level 2, check the <b>Enable Authentication Check Level-2</b> check box. <p>When enabled, packets that do not have the proper authentication are discarded. When disabled, IS-IS adds authentication to the outgoing packets, but does not check authentication on incoming packets, which allows for enabling authentication without disrupting the network operation.</p>
IS-IS Authentication KeyChain [Level 1 or Level-2]	Specify the key chain to be used for the authentication for corresponding level. The key chain can be up to 64 alphanumeric characters.

**Step 8** Click **Submit**.

To delete an IS-IS interface configuration, click the **Edit** icon for the interface, then click the **Delete** icon in the task bar.

**Step 9** Repeat [Step 5](#) through [Step 8](#) for each IS-IS interface.

- Step 10** To configure the MD-5 key chains for IS-IS, choose **Devices > Devices > Routing Settings > Proximity Server Settings > IS-IS > MD5 Settings**. The IS-IS Keychain page is displayed.
- Step 11** Click the **Create new KeyChain** icon. The Creating New KeyChain page is displayed.
- Step 12** In the **Key ID** field, enter the identifier for the keychain and click **Submit**. The page refreshes. The Key ID is identifier for the multiple key IDs that can be configured for the key chain.
- Step 13** Click the **Create New KeyChain Key** icon. The KeyChain Key page is displayed.
- Step 14** In the **Key ID** field, enter the key ID. The range is from 0 to 65535.
- Step 15** In the **Key String** field, enter the key string to be used for authentication. The key string can be up to 64 alphanumeric characters, except a space, single ('') and double quotes (""), and the "!" symbol.

## Configuring the OSPF Adjacencies

The Proximity OSPF page allows the Proximity Engine to establish an adjacency with its directly connected neighbor (router) to receive the whole LSDB content. Other OSPF settings depend on network topology, deployment and configuration of neighbor nodes.

OSPF is a link-state routing protocol for IGP. It runs on top of the IP protocol stack. Each node describes its neighbors in the link state advertisement (LSA) packets. The LSAs are flooded throughout the OSPF nodes. Each node uses shortest path first (SPF) to compute routes from the LSAs. The routes are then deposited into the RIB.



- Note** Only one IGP (IS-IS or OSPF) is supported for the Proximity Engine.

To configure the OSPF adjacencies, follow these steps:

- Step 1** Choose **Devices > Devices > Routing Settings > Proximity Server Settings > OSPF**. The Proximity OSPF page is displayed.
- Step 2** To enable OSPF adjacencies, check the **Enable** check box and click **Submit**. The Create new icons for Proximity OSPF Network, Proximity OSPF Area, and Proximity OSPF Interface icons display. To delete the OSPF configuration, click the **Delete** icon.
- Step 3** Check the **Enable log-adjacency-changes** check box to enable logging changes to the adjacency and click **Submit**. To delete the OSPF configuration, click the **Delete** icon.
- Step 4** To configure the proximity OSPF network, click the **Create new Proximity OSPF Network** icon. The Proximity OSPF Network page is displayed.
- Step 5** Enter the settings as appropriate. See [Table 4-56](#) for a description of the fields.

**Table 4-56 Proximity OSPF Network Fields**

Field	Description
IP Prefix	IP address that is used in combination with the <b>Network Mask</b> to produce the IP prefix. The IP prefix is used to define the OSPF area and consists of a combination of the IP address and netmask.
Wildcard Mask	Network mask is used with the <b>IP Prefix</b> to define the area on this network. The mask contains wild card bits where 0 is a match and 1 is a “do not care” bit, for example, 0.0.255.255 indicates a match in the first two bytes of the network number.
Area ID	<p>Identifier of the area for which IP prefix defines. The identifier can be specified as either a decimal value or an IP address. Valid entries are from 0 to 4294967295 or an IP address (A.B.C.D) can be used if you intend to associate areas with IP subnets.</p> <p>Each area is interface specific. For OSPF to operate on the OSPF interface, the primary address of the interface must be covered by the network area. The Proximity Engine sequentially evaluates the <b>IP Prefix/ Network Mask</b> pair for each interface as follows:</p> <ol style="list-style-type: none"> <li>1. The <b>Network Mask</b> is logically ORed with the OSPF interface IP address.</li> <li>2. The <b>Network Mask</b> is logically ORed with the <b>IP Prefix</b>.</li> <li>3. The software compares the two resulting values. If they match, OSPF is enabled on the associated interface and the associated OSPF interface is attached to the OSPF area specified.</li> </ol> <p>There is no limit to the number of network areas that can be configured.</p> <p><b>Note</b> An interface can only be associated to a single area. If the address ranges specified for different areas overlap, the software adopts the first area in the list and ignores the subsequent overlapping portions. In general, we recommend that you configure address ranges that do not overlap to avoid inadvertent conflicts.</p> <p>When a smaller OSPF network area is removed, the OSPF interfaces belonging to that network area are retained and remain active if a larger network area that encompasses those interfaces still exists. Interfaces that are part of a larger area are removed and become part of another area only if the other area is a smaller area (subset) of the larger area.</p>

**Step 6** Click **Submit**.

To delete an OSPF network configuration, click the **Edit** icon for the network, then click the **Delete** icon in the task bar.

**Step 7** Repeat **Step 4** through **Step 6** for each OSPF network.

To delete an OSPF network, click the OSPF network to display the settings and click the **Delete** icon.

**Step 8** To configure the proximity OSPF area, click the **Create new Proximity OSPF Area** icon. The Proximity OSPF Area page is displayed.**Step 9** Enter the settings as appropriate. See [Table 4-57](#) for a description of the fields.

**Table 4-57 Proximity OSPF Area Fields**

Field	Description
Area ID	Enter an Area ID that was defined in the Proximity OSPF Network page.
Type	<p>Choose one of the following area types:</p> <ul style="list-style-type: none"> <li>• NSSA (not-so-stubby area)—For areas that include an autonomous system boundary router (ASBR) that generates type 7 LSAs and an area border router (ABR) that translates them into type 5 LSAs.</li> <li>• Stub—An area with only one OSPF router that does not contain an ASBR.</li> </ul>

**Step 10** Click **Submit**.

To delete an OSPF area configuration, click the **Edit** icon for the area, then click the **Delete** icon in the task bar.

**Step 11** Repeat [Step 8](#) through [Step 10](#) for each OSPF area.

To delete an OSPF area, click the OSPF area to display the settings and click the **Delete** icon.

**Step 12** To configure the proximity OSPF network, click the **Create new Proximity OSPF Interface** icon. The Proximity OSPF Interface page is displayed.**Step 13** From the **Name** drop-down list, choose an interface to configure for OSPF. The number of available interfaces depends on the CDE.**Step 14** In the **OSPF Priority** field, enter the OSPF priority. The range is 0 to 255. The default is 1.

The highest OSPF priority on a segment becomes the designated router (DR) for that segment. A priority value of zero indicates an interface which is not to be elected as DR or backup designated router (BDR).

**Step 15** Click **Submit**.

To delete an OSPF interface configuration, click the **Edit** icon for the interface, then click the **Delete** icon in the task bar.

**Step 16** Repeat [Step 12](#) through [Step 15](#) for each OSPF interface.**Configuring the BGP Community-based Proximity Settings**

A BGP community is a group of prefixes that share some common property and can be configured with the BGP community attribute. The BGP community attribute is an optional transitive attribute of variable length. The attribute consists of a set of four octet values that specify a community. The community attribute values are encoded with an autonomous system (AS) number in the first two octets, with the remaining two octets defined by the AS. A prefix can have more than one community attribute. A BGP speaker that sees multiple community attributes in a prefix can act based on one, some, or all of the attributes.

See the “[BGP Proximity Algorithms](#)” section on page 1-50 for more information.

To configure the BGP community-based proximity settings, follow these steps:

**Step 1** Choose **Devices > Devices > Routing Settings > Proximity Server Settings > BGP**. The Proximity BGP page is displayed.**Step 2** In the **Local AS Number** field, enter the AS number that identifies the Proximity Engine and tags the routing information that is passed along.

AS numbers are globally unique numbers that are used to identify autonomous systems, and which enable an AS to exchange exterior routing information between neighboring autonomous systems. An AS is a connected group of IP networks that adhere to a single and clearly defined routing policy.

There are a limited number of available AS numbers. Therefore, it is important to determine which sites require unique AS numbers and which do not. Sites that do not require a unique AS number should use one or more of the AS numbers reserved for private use, which are in the range from 64512 to 65535.

**Step 3** Check the **Enable Log Neighbor Changes** check box to enable logging of status changes (up, down, or resets) to BGP neighbors.

Use the **show ip bgp neighbors** command to view the status changes.

**Step 4** Click **Submit**. The Create new icons for Location Community for BGP and Neighbor for BGP icons display.

To delete the BGP configuration, click the **Delete** icon.

**Step 5** To configure a BGP location community, click the **Create new Location Community for BGP**. The BGP Location Community page is displayed.



**Note** The maximum number of location communities allowed for each SE is 128. The **show running-config** command displays the location communities in ascending order.

**Step 6** In the **Location Community** field, enter the location community for the AS in one of the following formats:

<AS>:<POP>  
<AS1>:<POP1>-<AS2>:<POP2>

The location community numbers are used within the network to locate prefix origination points. The configuration includes all community values that represent a location. The **Location Community** field entry could be in the form of a list of community numbers, for example, 100:3535, 100:4566, 100:5678, 100:5678, 100:6789. Or, the community numbers can be expressed as intervals, such as 100:3000-100:4000, 100:5000-100:6000, and so on.

**Step 7** In the optional **Target Community** field, enter the target community that you want to associate with the Location Community.

If **Target Community** field is left blank, it is the same as the Location Community. So, if the target community is not specified, the PSA and PTA must have a common community for the PTA to be considered in the preference and ranking.

In certain deployments it is advantageous to include certain PTAs even though the PTAs do not share any community attributes with the PSA. A common example is an SE in a city close to the client PC; in such case, the SE might not share any community attributes with the client PC, but should be preferred over another SE in a far-away city. The **Target Community** field provides a way to associate PSA and PTA community attributes with each other and to assign a preference level (**Weight**) to that association.

The **Target Community** values have the same format and restrictions as the **Location Community** field, which are the following:

- Must match the pattern: <AS1>:<POP1>[-<AS2>:<POP2>]
- AS1 and AS2 must be in the range 1–65535.
- POP1 and POP2 must be in the range 0–65535.
- AS2 should be greater than AS1, or POP2 should be greater than POP1 if AS2 equals to AS1.
- New BGP community setting should make sure that target community and local community pair is unique and not existent.

**Note**

Source community ranges are not allowed to overlap. A maximum of 240 unique specific source or range source community configurations can be entered. Each unique specific source or range source community can be associated with a maximum of 240 unique specific target or range target communities.

- Step 8** In the optional **Weight** field, enter the weight to be assigned to the location community. The default is 1. The range is from 1 to 7 with 7 being the best association (most preferred). An association weight of 0 implicitly means no association (least preferred).

The weight is considered in the proximity ranking algorithm. If PTA1 and PTA2 have at least one community in common as the PSA, then the weight assigned to the location community is considered. The larger the number, the more weight the community has. If PTA1 has a weight of 5 and PTA2 has a weight of 2, PTA1 is preferred over PTA2.

- Step 9** Click **Submit**.

- Step 10** To configure a BGP neighbor, click the **Create new Neighbor for BGP**. The BGP Neighbor page is displayed.

- Step 11** Enter the settings as appropriate. See [Table 4-58](#) for a description of the fields.

**Table 4-58 BGP Neighbor Fields**

Field	Description
IP address	IP address of the neighbor.
Remote AS Number	AS number to which the neighbor belongs. The range is from 1 to 65535).
EBGP multihop TTL	Time-to-live value for the external BGP (eBGP) multihop scenarios. The range is from 2 to 255. The default is 1.
Keep Alive Interval	The keepalive interval, in seconds, for a BGP peer. The range is from 0 to 3600. The default is 60.
Hold Timer	The hold timer interval, in seconds, for a BGP peer. The range is from 0 to 3600. The default is 180.
Password	Enter the password to enable Message Digest 5 (MD-5) authentication on a TCP connection between the Proximity Engine and the BGP neighbor. The password is case sensitive and can be up to 79 characters. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format number-space-anything. The space after the number can cause authentication to fail.

To delete an BGP neighbor configuration, click the **Edit** icon for the neighbor, then click the **Delete** icon in the task bar.

- Step 12** Click **Submit**.

- Step 13** Repeat [Step 10](#) through [Step 12](#) for each BGP neighbor.

To delete a BGP neighbor, click the BGP neighbor to display the settings and click the **Delete** icon.

## Configuring SRP

The Service Routing Protocol (SRP) uses distributed hash table (DHT) technology to form a distributed network of Proximity Engines. For more information, see the “[Service Routing Protocol](#)” section on page 1-50.

**Note**

SRP is required if the Redirect proximity algorithm is enabled. SRP is used to gather and store information about all of the Proximity Engines that are available for redirection. See the “[Configuring the BGP Community-based Proximity Settings](#)” section on page 4-118 for more information.

To configure SRP, follow these steps:

**Step 1** Choose **Devices > Devices > Routing Settings > Proximity Server Settings > SRP**. The SRP page is displayed.

**Step 2** To enable SRP, check the **Enable** check box and click **Submit**. The Create new Bootstrap for SRP icon is displayed.

**Step 3** In the **Domain** field, enter a number that identifies the domain. The range is from 0 to 4294967295. The default is 0.

All Proximity Engines running SRP routing with the same domain ID form a single network if the nodes are found through a bootstrap node. By changing a Proximity Engine’s domain, the Proximity Engine leaves its current network.

We recommend that a domain ID value be configured for your DHT network so that all Proximity Engines that join this network share the same domain ID.

**Step 4** In the **Flooding Threshold** field, enter the maximum number of subscribers to flood or send messages to. The range is from 0 to 65535. The default is 50.

SRP uses flooding to send multicast messages for a multicast group if the number of subscribers in the group is equal to or more than the value specified in **Flooding Threshold**. An effective threshold value may improve protocol message overhead. The threshold value depends on the number of nodes in your DHT network. In general, the threshold value should be greater than half and smaller than 3/4 of the total number of DHT nodes in the network.

**Step 5** Click **Submit**.

To delete the SRP configuration, click the **Delete** icon.

**Step 6** To configure a SRP bootstrap, click the **Create new Bootstrap for SRP**. The Bootstrap SRP page is displayed.

**Step 7** In the **Bootstrap IP address** field, enter the IP address of the bootstrap node.

An IP address of a bootstrap node must be configured for each Proximity Engine before the Proximity Engine can join the network with others under the same domain ID. The first Proximity Engine in the network, which acts as the bootstrap node for others, does not need to configure itself as the bootstrap node; this is the only exception to configuring a bootstrap node. All other nodes must have the bootstrap node configured before they can join a DHT network. A maximum 25 bootstrap nodes are allowed per Proximity Engine. The port number for a bootstrap node is 9000.

**Step 8** Click **Submit**.

**Step 9** Repeat [Step 6](#) through [Step 8](#) for each bootstrap node.

To delete a bootstrap node, click the edit icon next to the IP address of the bootstrap node to display the settings and click the **Delete** icon.

---

## 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, follow these steps:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the SR that 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.
    - a. Check the **Enable Service Monitoring** 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 6** To enable the HTTP 302 redirection for Windows Media Technology files with an .asx extension, follow these steps:
    - a. Choose **Web > HTTP > HTTP Redirect**. The HTTP Redirect Settings page is displayed.
    - b. Check the **Enable HTTP 302 for .asx File** check box.
    - c. 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 Load Monitoring

For information on configuring all general settings, except load monitoring and last-resort routing, see the “General Settings” section on page 4-46.

Load monitoring provides the following functionality:

- Monitoring and aggregates of the load information of all SEs in the VDS-IS

- Monitoring and aggregates of all SEs assigned to a specific Delivery Service (domain)
- Minor alarms are raised when the monitored load exceeds the configured average or maximum threshold for all SEs in a Delivery Service or all SEs in the VDS-IS.

To configure load monitoring, follow these steps:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the SR that you want to configure. The Devices home page is displayed.
- Step 3** Click **Show All** to display the top-level menu options, and choose **General Settings > Notification and Tracking > CDS Monitor > General Settings**. The CDS Monitor General Settings page is displayed.
- Step 4** In the **Sample Period** field, enter the number of seconds between two consecutive samples. The sample period is the time during which the SE and the SR exchange keepalive messages that contain the device information. The default is 2. The range is from 1 to 300.
- Step 5** Check the **Enable** check box to enable load monitoring. If the Enable check box is not checked, the Streamer Settings and Domain Settings pages do not take effect.
- Step 6** Click **Submit**.
- Step 7** To enable the monitoring of all SEs in the CDS and configure the aggregate thresholds for the CDS, choose **Devices > Devices (SR) > General Settings > Notification and Tracking > CDS Monitor > Streamer Settings**. The CDS Monitor Settings page is displayed.
- Step 8** Enter the settings as appropriate. See [Table 4-61](#) for a description of the fields.

**Table 4-59 CDS Load Monitoring Fields**

Field	Description
Enable	<p>Check the <b>Enable</b> check box to enable load monitoring of all SEs in the CDS.</p> <p><b>Note</b> If the Enable check box is not checked on the CDS Monitor General Settings page, the Streamer Settings do not take effect.</p>
Device Average Threshold	Aggregate load value (as a percentage) of the average of all SEs in the CDS. This threshold defines the average device load of all of the SEs in the CDS. If the threshold is exceeded, an alarm is raised. The default is 80. The range is from 1 to 100.
Device Maximum Threshold	Aggregate load value (as a percentage) of the maximum of all SEs in the CDS. This threshold defines the maximum device load of all of the SEs in the CDS. If the threshold is exceeded, an alarm is raised. The default is 80. The range is from 1 to 100.

- Step 9** Click **Submit**.
- Step 10** To enable monitoring of specific delivery services (domains) and configure the aggregate thresholds for each domain, choose **Devices > Devices (SR) > General Settings > Notification and Tracking > CDS Monitor > Domain Settings**. The Domain Monitor Table page is displayed.
- The table is sortable by clicking the column headings.
- Step 11** Click the **Create New** icon.
- Click the **Edit** icon next to the domain name to edit a table entry.
- Step 12** Enter the settings as appropriate. See [Table 4-60](#) for a description of the fields.

**Table 4-60 Domain Load Monitoring Fields**

Field	Description
Domain Name	The service routing fully qualified domain name (RFQDN) (for example, srfqdn.cisco.com) configured for the Delivery Service.
Enable	<p>Check the <b>Enable</b> check box to enable load monitoring of this domain.</p> <p><b>Note</b> If the Enable check box is not checked on the CDS Monitor General Settings page, the Domain Settings do not take effect.</p>
Device Average Threshold	Aggregate load value (as a percentage) of the average of all SEs in the CDS. This threshold defines the average device load of all of the SEs in the CDS. If the threshold is exceeded, an alarm is raised. The default is 80. The range is from 1 to 100.
Device Maximum Threshold	Aggregate load value (as a percentage) of the maximum of all SEs in the CDS. This threshold defines the maximum device load of all of the SEs in the CDS. If the threshold is exceeded, an alarm is raised. The default is 80. The range is from 1 to 100.

**Step 13** Click **Submit**. The entry is added to the Domain Monitor Table.

To delete a load monitoring configuration for a domain, click the **Edit** icon for the domain, then click the **Delete** icon in the task bar.

## Configuring Last-Resort Routing

For information on configuring all general settings, except load monitoring and last-resort routing, see the “General Settings” section on page 4-46.



**Note** When DNS-based redirection is used, for application-level requests, last-resort redirection is supported. However, on the DNS plane, an A record with the last-resort domain name or IP address is not returned.

Last-resort routing is useful when all Service Engines have exceeded their thresholds, all Service Engines in the domain are offline, no Service Engines have been assigned to a particular domain, or the client is unknown. If last-resort routing is configured, the Service Router redirects requests to a configurable alternate domain or translator response 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 (for location-based routing) listed in the Coverage Zone file.

Last-resort routing could also be configured to redirect a client to an error domain and filename.

The URL translator provides a way to dynamically translate the client request URL to redirect the client to a different CDN. With the URL translator option, the following occurs if the SR uses last-resort routing for a client request:

1. The SR contacts the third-party URL translator through the Web Service API. The Web Service API is described in the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 API Guide*.
2. The third-party URL translator sends the translated URL in the response to the SR.

3. The SR sends a 302 redirect message to the client with the translated URL it received from the third-party URL translator.

The timeout for connecting to the URL translator server is 500 milliseconds. There are no retries if the URL translator cannot be reached.

If there is no configuration on the URL translator for the requested domain or the connection timeout threshold has been reached, the SR last-resort routing falls back to the alternate domain configuration.

For more information, see the “[Last-Resort Routing](#)” section on page 1-42.


**Note**

If the last-resort domain or the translator response domain are not configured and the Service Engine thresholds are exceeded, known client requests are redirected to the Origin server (if Enable Origin Server Redirect is enabled) and unknown clients 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) or translator response 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.

To configure last-resort routing, follow these steps:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the SR that you want to configure. The Devices home page is displayed.
  - Step 3** Click **Show All** to display the top-level menu options, and choose **General Settings > Last Resort**. The Last Resort Table page is displayed.  
The table is sortable by clicking the column headings.
  - Step 4** Click the **Create New** icon.  
Click the **Edit** icon next to the domain name to edit a table entry.
  - Step 5** Enter the settings as appropriate. See [Table 4-61](#) for a description of the fields.

**Table 4-61      Service Router Last Resort Fields**

Field	Description
Domain Name	The service routing fully qualified domain name (RFQDN) (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>

**Table 4-61** Service Router Last Resort Fields (continued)

Field	Description
Alternate Domain Name	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.
Alternate Domain Port	If an <b>Alternate Domain Name</b> is not specified, requests for the domain entered in the Domain Name are routed to the Origin server.  The <b>Alternate Domain Name</b> could be a domain outside the VDS-IS. 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.  To specify a different port than the default (80), enter the port number in the <b>Alternate Domain Port</b> field. Default is 80. Range is from 1 to 65535. Well-known port numbers are not allowed. For the list of well-known ports, see the “ <a href="#">System Port Numbers</a> ” section on page 8-10.
Error Domain Name	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.
Error Domain Port	The <b>Error Domain Name</b> could be a domain outside the VDS-IS. 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.  To specify a different port than the default (80), enter the port number in the <b>Error Domain Port</b> field. Default is 80. The range is from 1 to 65535. Well-known port numbers are not allowed. For the list of well-known ports, see the “ <a href="#">System Port Numbers</a> ” section on page 8-10.
Error File Name	The filename of the error URL (for example, error.html or error/errorfile.flv).  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.  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.  <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>rtmp://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.
Translator IP address	IP address of the URL translator server. If there is no configuration on the URL translator for the requested domain or the connection timeout threshold has been reached, the SR last-resort routing falls back to the alternate domain configuration.
Translator Port	To specify a different port than the default (80), enter the port number in the <b>Translator Port</b> field. Default is 80. The range is from 1 to 65535. Well-known port numbers are not allowed. For the list of well-known ports, see the “ <a href="#">System Port Numbers</a> ” section on page 8-10.

**Step 6** 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.

As an example configuration for an error URL to redirect unknown clients to or to redirect clients to when all SEs in the Delivery Service are unavailable follows:

- 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>.

To be more specific, 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

It is important to remember that when redirecting a client request for live Windows Media Streaming programs because live programs deliver an ASX file to the client, the error message must have the same format. 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, the following is a simple ASX file:

```
<ASX VERSION="3.0"> <Entry>

<REF HREF="http://<IP-Address-of-Server/path/filename"/>

</Entry> </ASX>
```

If you want 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 the following:

```
<ASX VERSION="3.0"> <Entry>

<REF HREF="http://3.1.1.1/vod/testMessage.gif"/>

</Entry> </ASX>
```

There are other ways to use an ASX file to display information. The following 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/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 Domain Subscription

The Domain Subscription page allows you to subscribe the SR to specific domains. By default, the SR takes all of the domains specified in the CDSM. By specifying the domains in the Domain Subscription page, the SR only subscribes to the assigned content origins.

- 
- Step 1** Choose **Devices > Devices > General Settings > Domain Subscription**. The Domain Subscription page displays all defined content origins of the VDS-IS.
- Step 2** Click the **Assign** icon (blue cross mark) next to the Content Origin that you want to assign to this SE. Alternatively, click the **Assign All Content Origins** icon in the task bar.

A green arrow wrapped around the blue X indicates a content origin assignment is ready to be submitted. To unassign a Content Origin, click this icon. The Content Origin assignment states are described in [Figure 4-14](#).

**Figure 4-14 Content Origin Assignment State**

New Assign	Assigned and waiting for Submit	Assignment Submitted	Unassign Assignment

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

A green circle with a check mark indicates a Content Origin is assigned to this SR. To unassign the Content Origin, click this icon, or click the **Remove All Content Origins** icon in the task bar. Click **Submit** to save the changes.

Additionally, the **Filter Table** icon and **View All Content Origins** icon allow you to first filter a table and then view all content origins again.

---

## Configuring Memory Limitation Settings

To configure the memory limitation settings for an SR, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Memory Limitation**. The Memory Limitation page is displayed.
- Step 2** Enter the settings as appropriate. See [Table 4-62](#) for a description of the fields.

**Table 4-62 Memory Limitation Settings Fields**

Field	Description
service-router	Memory size for Service Router. The default value is 4GB.
fms-server	Memory size for Flash Media Server. If the physical memory size is greater or equal to 48GB, the default value will be 8GB. If the physical memory size is between 48GB and 32GB, the default value is 6GB, otherwise the default value is 4GB.

**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 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 8-89.

To enable transaction logging for the SR, follow these steps:

**Step 1** Choose **Devices > Devices > General Settings > Notification and Tracking > Transaction Logging**. The Transaction Log Settings page is displayed.

**Step 2** Enter the settings as appropriate. See [Table 4-63](#) for a description of the fields.

**Table 4-63 Transaction Log Settings Fields**

Field	Description
<b>General Settings</b>	
Transaction Log Enable	Enables transaction logging.
Snapshot Counter Log Enable	Enables the Snapshot Counter transaction log. For more information, see the “ <a href="#">Snapshot Counter Transaction Logs</a> ” section on page 8-100.
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 500,000.
Max number of files to be archived	Maximum number of files to be maintained on the local disk. The range is from 1 to 10,000. The default is 10.

**Table 4-63 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.
Skip Log Types	Enables to skip exporting of specific transaction logs. By default, no log type chosen to skip export.
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.

**Table 4-63 Transaction Log Settings Fields (continued)**

Field	Description
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.
FTP Export IPv6 Server	IPv6 address or hostname of the FTP server.
<b>Splunk UF Export Settings</b>	
Export Enable	Enables the automatic export of the selected transaction logs to the designated export server. For more information, see the “ <a href="#">Real-Time Exporting of Transaction Logs for Billing and Analytic Reports</a> ” section on page 8-102.
Monitors	Check the check boxes of the type of transaction logs to export. The <b>All</b> check box means all transaction logs are exported.
Export Server and Port	IP address and port number of the CDNM, CDN, or other export server that is to receive the transaction log files. A maximum of three export servers can be specified. The default port number is 9998.

**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 CDSM

Configuring a CDSM consists of the General Settings menu items. For information on configuring general settings, see the “[General Settings](#)” section on page 4-46.

Device activation is accomplished during installation and initialization of the VDS-IS devices. See *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide* for more information.

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, enter a new name in the **Name** field and click **Submit**.

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





## Configuring Services

This chapter describes how to configure services for the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS).

- [Configuring Delivery Services, page 5-1](#)
- [Configuring Programs, page 5-47](#)
- [Viewing Programs, page 5-59](#)
- [Copying a Program, page 5-62](#)

## 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 1-3.

Configuring a Delivery Service consists of defining the following:

- [Content Origins, page 5-1](#)
- [Creating Multicast Clouds, page 5-8](#)
- [Creating Storage Priority Classes, page 5-15](#)
- [Creating Delivery Service, page 5-16](#)
- [Identifying Content, page 5-33](#)

## 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 2-9.



**Note** When VOD (prefetch/caching) and live streaming share the same content origin, and the Service Rules XML file is configured to validate the signed URL where the domain must match the Service Routing Domain Name, make sure to create rule patterns for the URL validation to match both the Service Routing Domain Name and the Origin Server FQDN. Additionally, when the URL is signed, exclude the domain from the signature. See the “[Running a Python URL Signing Script](#)” section on page H-11 for more information. The URL validation must not include the domain for validation (use the **exclude-domain** option for the *exclude-validate* attribute of the **Rule\_Validate** element). See the “[Service Rule File Structure and Syntax](#)” section on page E-4 for more information.

To create a Content Origin, follow these steps:

- Step 1** Choose Services > Service Definition > Content Origins. The Content Origin Table page is displayed (Figure 5-1).

**Figure 5-1 Content Origin Table**

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 5-1).

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

- Step 3** Enter the settings as appropriate. See Table 5-1 for a description of the fields.

**Table 5-1 Content Origin Fields**

Field	Description
Name	Unique name of the origin server.
Origin Server	<p>Origin fully qualified domain name (OFQDN) of the origin server or IPv6 or IPv4 address. To support Origin server redirection for IPv6 clients and dual-stack clients, do not use the IP address of the Origin server when configuring the content origin for a Delivery Service; instead, use the domain name associated with the origin server.</p> <p><b>Note</b> The string “.se.” cannot be used in the OFQDN.</p>
Service Routing Domain Name	<p>The FQDN used to route client requests. The SE translates the service routing FQDN (SRFQDN) to the origin server whenever it needs to retrieve content from the origin server.</p> <p><b>Note</b> The string “.se.” cannot be used in the SRFQDN.</p> <p>The service routing domain name configured for the content origin should also be configured in the DNS servers, so that 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>
NAS Configuration File	<p>From the <b>NAS Configuration File</b> drop-down list, choose a NAS file.</p> <p>The <b>NAS Configuration File</b> drop-down list is populated with the NAS files that are registered to the CDSM. See the “<a href="#">NAS File Registration</a>” section on page 6-16 for information on registering a NAS file.</p> <p>A NAS file is an XML file that specifies the parameters for the Network Attached Storage (NAS) device. For information on creating a NAS file, see <a href="#">Appendix G, “Creating NAS Files.”</a></p> <p><b>Note</b> NAS is only supported in lab integrations as proof of concept.</p>
Enable Content Based Routing	<p>Check the <b>Enable Content Based Routing</b> check box to enable content-based routing for this content origin. Content-based routing is enabled by default.</p> <p><b>Note</b> This option requires that content-based routing be enabled on the SR. See the “<a href="#">Configuring Request Routing Settings</a>” section on page 4-104.</p>
Enable Origin Server Redirect	<p><b>Enable Origin Server Redirect</b> (which is the default) means the last-resort routing behavior does not change. When <b>Enable Origin Server Redirect</b> is disabled any client request for the Origin server (domain) is never redirected to the Origin server and receives a 404 “not found” message instead.</p> <p>For more information about last-resort routing, see the “<a href="#">Last-Resort Routing</a>” section on page 1-42. To configure last-resort routing, see the “<a href="#">Configuring Last-Resort Routing</a>” section on page 4-124.</p>

**Table 5-1 Content Origin Fields (continued)**

Field	Description
Windows Media Authentication Type	The type of client authentication that is required by the origin server. The options are as follows: <ul style="list-style-type: none"> <li>• None</li> <li>• Basic authentication</li> <li>• NTLM authentication</li> <li>• Digest</li> <li>• Negotiate</li> </ul>
HTTP Authentication Type	HTTP Authentication provides a way for the Origin server to authenticate HTTP requests by one of the following methods: <ul style="list-style-type: none"> <li>• <b>Basic Authentication</b></li> <li>• <b>Challenged Authentication</b></li> </ul> Choose <b>None</b> to not configure HTTP Authentication. For more information, see the “Custom HTTP Header Authentication for Origin Server” section on page 5-6.
Comments	Information about the content origin.



**Note** The string “.se.” cannot be used in the SRFQDN and OFQDN.

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

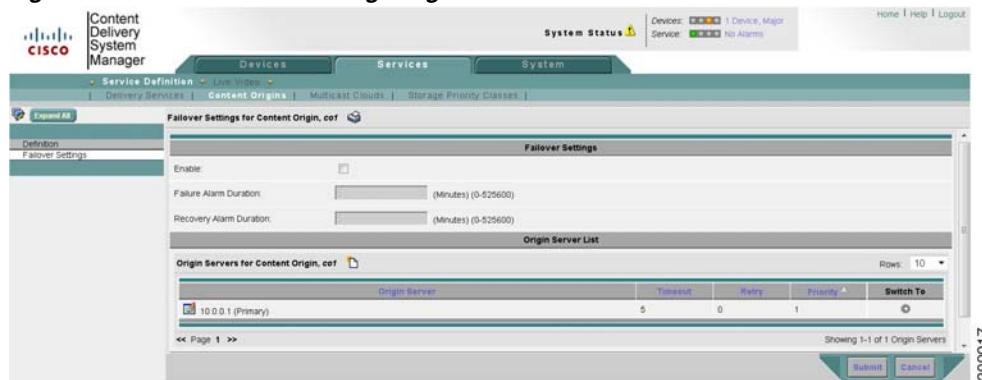
To delete a Content Origin, from the Content Origin Table page, click the **Edit** icon next to the Content Origin that you want to delete, and click the **Delete** icon in the task bar.



**Caution** Do not delete a content origin that has a Delivery Service associated to it. First delete the Delivery Service associated with the content origin, then delete the content origin.

## Enabling OS Failover Support for Content Origin

- Step 1** Choose **Services > Service Definition > Content Origins**. The Content Origin Table page is displayed ([Figure 5-1](#)).
- Step 2** Click the **Edit** icon next to the Content Origin name. The Content Origin Information page is displayed.
- Step 3** Click **Failover Settings** ([Figure 5-2](#)). Enter the settings as appropriate. See [Table 5-2](#) for a description of the fields.

**Figure 5-2** Failover Settings Page**Table 5-2** Failover Settings Fields

Field	Description
<b>Failover Settings for Content Origin</b>	
Enable	Check the <b>Enable</b> check box to enable OS Failover support for this content origin. OS Failover Support is disabled by default.
Failure Alarm Duration	Determines the duration (in minutes) to retain the failure alarm. The default value is 5 minutes. The range is from 0 to 525600 minutes. <b>Note</b> When it is set to 0, it means this alarm will not be raised.
Recovery Alarm Duration	Determines the duration (in minutes) to retain the recovery alarm. The default value is 5 minutes. The range is from 0 to 525600 minutes. <b>Note</b> When it is set to 0, it means this alarm will not be raised.

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

#### Origin Servers List for Content Origin

Origin Server	FQDN or IPv6 or IPv4 address of the Origin Server.
Timeout	Connection timeout of the Origin Server.
Retry	The number of retry times when the connection to Origin Server fails.

Priority	The order of Origin Server switching during failover.
Switch To	<p>Click <b>Switch To</b> to manually switch to the corresponding Origin Server.</p> <p><b>Note</b> The <b>Switch To</b> button is enabled only when OS Failover is enabled.</p>

- a. To add a new Origin server for the content origin, click the **Create New** icon next to the Origin Servers for the content origin.
- b. Enter the settings as appropriate. See [Table 5-3](#) for a description of the fields.

**Table 5-3** *New Origin Server List Fields*

Field	Description
Origin Server	FQDN or IPv6 or IPv4 address of Origin Server.
Timeout	Connection timeout of the Origin Server. The default value is 5 seconds. The range is from 1 to 255 seconds.
Retry	The number of retry times when the connection to Origin Server fails. The default value is 0. The range is from 0 to 255.
<b>Note</b>	When it is set to 0, it means that there are no retries when the connection fails.
Priority	The order of Origin Server switching during failover. The default value is 500. The range is from 1 to 1000.
<b>Note</b>	Value 1 indicates highest priority and value 1000 indicates lowest priority.

- c. Click **Submit** to save the settings for new Origin Server.

To edit the Origin Server for Content Origin, click the **Edit** icon next to the Origin Server Name in the Failover Settings page and modify the settings.

To delete the Origin Server for Content Origin, click the **Edit** icon next to the Origin Server Name in the Failover Settings page, the Origin Server Definition page is displayed. Click the **Trash** icon in the task bar.

## Custom HTTP Header Authentication for Origin Server

Custom HTTP Header Authentication provides a way for the Origin server to authenticate HTTP requests by the following methods:

- [Basic HTTP Header Authentication, page 5-7](#)
- [Challenged HTTP Header Authentication, page 5-7](#)

**Note**

If a Manifest file is located on an Origin server that requires custom HTTP header authentication, fetching the Manifest file by using the **Specify external manifest file** method fails. The Manifest file must be located on a server that does not require custom HTTP header authentication.

**Note**

Custom HTTP Header authentication supports HTTP 302 redirection. But the authentication process could only be used for the first server. It is not supported for the redirected destination server.

**Note**

If OS failover is enabled, custom HTTP header authentication is not supported for alternate OS.

### Basic HTTP Header Authentication

The basic HTTP header authentication method uses a shared key between the Origin server and the Content Acquirer of the Delivery Service. Each HTTP request to the Origin server includes the shared key in the HTTP header. If **Basic Authentication** is selected from the **HTTP Authentication Type** drop-down list, the following fields are displayed:

- **HTTP Authentication Header**—Name of the HTTP authentication header.
- **HTTP Authentication Shared Key**—Shared key. The shared key must be at least 16 characters and must be composed of TEXT characters defined in RFC 2616 HTTP/1.1. The range is from 16 to 128 characters.

### Challenged HTTP Header Authentication

The challenged HTTP header authentication method uses a shared secret key between the Origin server and the Content Acquirer of the Delivery Service. The authentication message does not display the secret key. The shared secret key uses a random challenge string and cryptographic hash algorithm.

The random challenge string is composed of TEXT characters defined in RFC 2616 HTTP/1.1 and is the same length as the secret key. Following is the process that occurs for the challenged HTTP header authentication method:

1. A binary XOR between the challenge string and the secret key is created.
2. The authentication value is created by using the cryptographic hash of the XOR value.
3. The following authentication headers are added to the HTTP request that is sent to the Origin server:
  - Header with challenge string
  - Header with authentication value
4. The hashing algorithm is implemented and the name of the hashing function is included in the HTTP header.
5. The prefix name (identified as HPFX in this scenario) of the authentication HTTP header is used to construct the following header names:
  - Challenge string header—HPFX-CSTR
  - Authentication value header—HPFX-AUTH
  - Hashing function header—HPFX-HASH
6. When the Origin server receives the request, it must follow these steps:
  - a. Compute a binary XOR between the HPFX-CSTR header value and the secret key configured in the VDS-IS.

- b. Compute the authentication value with the cryptographic hash in the HPFX-HASH header.
- c. Grant access if the Origin server computed authentication value and the authentication value header (HPFX-AUTH) match (both are lowercase).

If **Challenged Authentication** is selected from the **HTTP Authentication Type** drop-down list, the following fields are displayed:

- **HTTP Authentication Header Prefix**—Prefix of the HTTP authentication header.
- **HTTP Authentication Shared Secret Key**—Shared secret key. The shared secret key must be at least 16 characters and must be composed of TEXT characters defined in RFC 2616 HTTP/1.1. The range is from 16 to 128 characters.
- **HTTP Authentication Hashing Function**—Hashing algorithm for the shared secret key. Choose **MD5**.

## Creating Multicast Clouds

A Multicast Cloud is created by specifying an IP multicast address for advertising the data being transferred, an IP multicast address range for transferring the data, a primary multicast sender SE and an optional backup sender, a set of receiver SEs, and a maximum rate at which to send the data.

**Note**

The Multicast Cloud feature is supported in all releases starting with Release 3.1.1.

**Note**

We highly recommend that you avoid using multicast addresses of the form x.0.0.y (for example, 238.0.0.1). These addresses hash to the same Ethernet address space as 224.0.0.x, which is used frequently by routers and switches for local multicasts. Additional traffic on these addresses adds to the workload of these network elements.

To create a Multicast Cloud, follow these steps:

- 
- Step 1** From the CDSM GUI, choose **Services > Service Definition > Multicast Clouds**. The Multicast Clouds Table page is displayed.
  - Step 2** Click the **Create New** icon in the task bar. The Multicast Cloud Definition page is displayed.  
To edit a Multicast Cloud, click the **Edit** icon next to the Multicast Cloud name.
  - Step 3** Enter the settings as appropriate. See [Table 5-4](#) for a description of the fields.

**Table 5-4 Multicast Cloud Fields**

Field	Description
<b>Multicast Cloud Information</b>	
Name	Identifier for the Multicast Cloud. The name must be unique across the system.
Advertisement IP address	Unique advertisement address provides all of the SEs in one cloud with the same advertisement address and allows them to communicate multicast session information. The advertisement IP address must conform to these guidelines: <ul style="list-style-type: none"> <li>• It must be unique across the system.</li> <li>• It must be within the RFC multicast range (224.0.0.0–239.255.255.255).</li> <li>• It must not be within the start and end range specified by this cloud.</li> </ul>
Port	Port used for file addresses. The default port is 7777.  The allowed multicast port range is 1 through 65535. However, the multicast-enabled network may impose certain restrictions on your choice of port. Normally, port numbers below 1024 should be avoided, but the SE does not enforce any restrictions.
<b>Multicast Address Settings</b>	
Start IP address	The multicast address range is used to provide each Delivery Service associated with it a unique multicast address. When you assign a Multicast Cloud to a Delivery Service, an unused IP address is automatically selected from this range to ensure that the address is used by only one Delivery Service and by only one Multicast Cloud.  The <b>Start IP address</b> is the start of the IP address range, which must be within the range 224.0.0.0 to 239.255.255.255.  The IP address range must conform to the following: <ul style="list-style-type: none"> <li>• IP address range cannot overlap with program multicast addresses.</li> <li>• IP address range must contain all multicast addresses used by this cloud with its associated Delivery Service.</li> </ul> <p><b>Note</b> The IP address range in one Multicast Cloud can overlap that of another Multicast Cloud. A message alerts you if there is an overlap, but allows the operation. You must choose a multicast IP address that does not conflict internally within the same multicast-enabled network configuration. This multicast IP address is not related to the IP address of the SE.</p>
End IP address	End of the IP address range, which must be higher than the start IP address. The end IP address must be within the range 224.0.0.0 to 239.255.255.255.
Default Multicast-out Bandwidth	Maximum multicast rate in kilobits per second (Kbps). This value applies to the sender SE 24 hours a day, 7 days a week. The minimum rate is 10 Kbps.  To customize bandwidth rates for different days, use the Replication Scheduled Bandwidth page. The settings on the Replication Scheduled Bandwidth page override the <b>Default Multicast-out Bandwidth</b> field for the period specified in the Replication Scheduled Bandwidth page. For more information, see the “Replication” section of the “Configuring Devices” chapter in the <i>Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Software Configuration Guide</i> .
Synchronize Primary and Backup SE Multicast-out Bandwidth	When checked, <b>Default Multicast-out Bandwidth</b> settings are used by both primary and backup senders, if a backup sender is configured.

**Table 5-4 Multicast Cloud Fields (continued)**

Field	Description
Backup SE Default Multicast-out Bandwidth	Maximum multicast rate in kilobits per second (Kbps) for the backup sender. The minimum rate is 10 Kbps.
Default Delivery Service Multicast-out Bandwidth	This value is used when, the bandwidth value is not provided while the Multicast Cloud is assigned to a Delivery Service.
Maximum concurrent Sessions	Maximum number of jobs that are scheduled concurrently for the Multicast Cloud.
<b>Advanced Settings</b>	
Multicast medium	Means of transmitting the multicast, either <b>Satellite</b> or <b>Terrestrial</b> . The default is <b>Satellite</b> .
# of Carousel passes	<p>Maximum number of times that a multicast sender attempts to send missing content for on-demand carousels. The range is from 1 to 1000000000 (1 billion). The default is 5.</p> <p><b>Note</b> If the multicast sender finishes the last carousel on an object at time <math>t</math> and the multicast sender receives a NACK within <math>t + \text{carousel\_delay}</math>, the multicast sender starts the next carousel of this object at time <math>t + \text{carousel\_delay}</math>. That is, the multicast carousel is not triggered immediately upon receipt of a NACK if the carousel delay (<b>Delay between passes</b> field) is greater than zero (0).</p> <p>For more information, see the “<a href="#">Configuring Carousel Passes</a>” section on page 5-11.</p> <p><b>Note</b> If the number of carousel passes configured is used up, the syslog displays a warning message as an alert.</p>
TTL	Number of hops (Time to Live [TTL]) a packet travels before it is discarded, regardless of whether or not the packet has reached its destination. The range is from 1 to 255. The default is 255.
Delay between passes	Delay, in minutes, between file transmissions. The range is from 0 to 10080 (one week). The default is 0.
FEC transmission group	<p>Size of the FEC (forward error correction) block in packets. (See RFC 3208 <i>PGM Reliable Transport Protocol Specification</i> for more information.) The allowable inputs are 2, 4, 8, 16, 32, 64, and 128. The default is 16.</p> <p>FEC data encoding protects transmissions against errors, without requiring retransmission. The FEC number denotes the number of packets that is encoded into one FEC transmission group. When the FEC number goes up, the transmission group becomes larger, so the multicast may be more error-resistant. However, there is more computational overhead and bandwidth usage on the multicast sender and receivers.</p> <p>For more information, see the “<a href="#">Multicast Forward Error Correction and Proactive Forward Error Correction</a>” section on page 2-15.</p>
FEC proactive parity size	The value for the <b>FEC proactive parity size</b> field cannot be greater than the FEC Transmission Group value. The default is 2.
FEC proactive parity delay	The value is represented in milliseconds. The default is 1 millisecond.
PGM Router-assist	Specifies whether IP routers are to be used to assist in distribution of content. To enable the IP router alert option for Pragmatic Group Multicasting (PGM) packets, check the <b>PGM Router-assist</b> check box.
Primary-to-backup failover grace period	Amount of time (in minutes) allotted for the backup sender to detect whether the primary sender is active. If the backup sender does not hear a heartbeat from the primary sender within this grace period, the backup sender assumes the active role. The range is from 5 to 7200. The default is 30.

**Table 5-4 Multicast Cloud Fields (continued)**

Field	Description
Backup-to-primary fallback grace period	Amount of time (in minutes) allotted for the primary sender to detect whether the backup is active. If the backup sender does not respond within this grace period, the primary sender assumes the active role. The range is 5–7200. The default is 30.
Comments	Comments about the Multicast Cloud.

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

---

To delete a Multicast Cloud, click the **Edit** icon next to the Multicast Cloud that you want to delete, the Multicast Cloud Definition page is displayed. Click the **Trash** icon in the task bar.

## Configuring Carousel Passes

The number of carousel passes is the maximum number of times a multicast sender can retransmit the multicast for missing files. The primary sender sends the first carousel pass automatically. After the first round, multicast receiver SEs request missing content by sending a negative acknowledgment (NACK) to the sender that identifies the missing content. Late-joining receivers or receivers that missed some content send a NACK to the sender for any files that were not received. The multicast sender sends out the requested content when it receives the NACK from the receiver. After all receiver SEs have received all of the multicast content or the sender has reached the maximum number of carousel passes, whichever comes first, the sender stops transmitting content.

The **multicast fixed-carousel enable** command enables fixed-carousel sending. By default, the SE uses intelligent carousel sending, which means that the retransmission is guided by feedback from the multicast receivers in the form of NACKs. Fixed-carousel sending causes the content to be sent without depending on any receiver feedback. When this feature is enabled, the SE continuously retransmits the content after waiting the time specified by the **sender-delay** option. This configuration is allowed only for the primary sender and is not supported on the backup sender.

If the primary sender fails and the backup sender becomes active, the backup sender takes charge of NACK processing. The backup sender's carousel passes are always triggered by a NACK. When the maximum number of carousel passes is reached for a file on the current active sender, if the Delivery Service is configured with the **Multicast Unicast**, file distribution falls back to unicast. See the “[Multicast Replication](#)” section on page 2-13.

The Delivery Service can be set to fall back to unicast (Multicast Unicast Option set to **Multicast Unicast**) after the maximum number of carousel passes has been reached. If the administrator wants the SEs to fall back to unicast (for example, with a multi-tier unicast deployment using a terrestrial multicast medium), the Multicast Cloud should be configured for a low number of carousel passes (such as 1, 2, or 3).

If multicast replication is preferred (for example, with a hub and spoke or star topology deployment using a satellite multicast medium), use a high number of carousel passes, such as 10 or more.

To adjust the pacing of the multicast transmission, you can specify how much time must elapse before missing files are resent (the **Delay between passes** field on the Multicast Cloud Definition page).

Starting with Release 3.2.2, VDS-IS supports configuring carousel passes at Delivery Service level via **Services > Service Definition > Delivery Services > Assign Multicast Clouds to Delivery Service** page in CDSM GUI. The carousel passes configured for each Delivery Service will override the carousel

passes configured at the global Multicast Cloud level. The number of carousel passes configured for each Delivery Service level must be greater than 0 and less than or equal to the number of carousel passes configured at the global Multicast Cloud level.

The SE will fall back to unicast transmission if the number of carousel passes configured for a Delivery Service gets exhausted. Delivery service carousel value will hold same value as global Multicast Cloud carousel value, if carousel value remains unchanged at Delivery Service multicast configuration.

## Assigning SEs to a Multicast Cloud

To add SEs to a Multicast Cloud, follow these steps:

- Step 1** From the CDSM GUI, choose **Services > Service Definition > Multicast Clouds**. The Multicast Clouds page is displayed.
- Step 2** Click the **Edit** icon next to the name of the Multicast Cloud that you want to assign sender and receiver SEs to. The Multicast Cloud Definition page is displayed.
- Step 3** From the left-panel menu, click **Assign Service Engines**. The Service Engine Assignment page is displayed.
- Step 4** Assign the SEs to the Multicast Cloud by selecting a role (receiver, primary sender, and backup sender) for each SE. [Table 5-5](#) describes the SE role assignments for a Multicast Cloud.
  - a. From the **Role** drop-down list, choose **Primary Sender**, click the **Assign** icon (blue cross mark) next to the SE that is the primary sender for the Multicast Cloud, and click **Submit**.  
The SE states are described in [Figure 5-3](#).
  - b. From the **Role** drop-down list, choose **Backup Sender**, click the **Assign** icon next to the SE that is the backup sender for the Multicast Cloud, and click **Submit**.
  - c. From the **Role** drop-down list, choose **Receiver**, click the **Assign** icon next to the SE that is a receiver for the Multicast Cloud, and click **Submit**.

Alternatively, click the **Assign all Service Engines** icon in the task bar to assign all remaining SEs as multicast receivers to the Multicast Cloud and click **Submit**.



**Note** Everytime a primary/backup sender is assigned/deassigned to a cloud, the mcast\_sender process restarts to process the new cloud details.



**Note** The CDSM GUI allows you to assign SEs that are not multicast enabled. However, you must ensure that any SE that you assign to a Multicast Cloud is multicast enabled. (See the “[Enabling SEs for Multicasting](#)” section on page 4-20.)

**Figure 5-3 SE Assignment State**

New Assign	Assigned and waiting for Submit	Assignment Submitted	Unassign Submitted Assignment	Not modifiable.	209850

**Table 5-5 SE Role Assignments for Multicast Clouds**

Role Assignment	Description
Primary sender	<p>Primary SE that pushes content to a set of SE receivers using multicast. A Primary sender cannot be the following:</p> <ul style="list-style-type: none"> <li>• Backup sender or Receiver for the same cloud.</li> <li>• Primary sender or Backup sender for a different cloud.</li> </ul> <p>A sender SE cannot be deleted from the network. Before deleting a sender SE, you must choose another SE as the sender for the Multicast Cloud.</p>
Backup sender	<p>Backup sender SE that takes over in the event of failure of the Primary sender. A Backup sender cannot be the following:</p> <ul style="list-style-type: none"> <li>• Primary sender or Receiver for the same cloud.</li> <li>• Primary sender or Backup sender for a different cloud.</li> </ul> <p>The Primary and Backup senders of a Multicast Cloud should subscribe to the same set of multicast-enabled delivery services.</p>
Receiver	<p>SEs that receive content from the Primary sender. Use the following guidelines when adding receiver SEs:</p> <ul style="list-style-type: none"> <li>• Multicast cloud must have at least one Receiver. To create a functional Multicast Cloud, you must add at least one receiver SE.</li> <li>• Maximum number of receivers that can be added is the total number of SEs in the system (excluding the sender SE).</li> <li>• Receiver cannot be a receiver in another Multicast Cloud.</li> <li>• Receiver cannot be a sender in the same Multicast Cloud. Only SEs that are not assigned to another Multicast Cloud are displayed in the Service Engine Assignment page.</li> <li>• Content Acquirer for the Delivery Service cannot be a receiver in the Multicast Cloud.</li> <li>• Only a fully configured Multicast Cloud (with at least one receiver SE) can be assigned to a Delivery Service to enable multicast capability.</li> </ul>

To remove an SE from the Multicast Cloud, click the **Unassign** icon next to the SE that you want to remove, and click **Submit**. Alternatively, to remove all receiver SEs, you can click the **Remove all Service Engines** icon in the task bar and click **Submit**. After you click **Submit**, a blue cross mark appears next to the unassigned SE.

### Configuring the Multicast Sender Delay Interval

The multicast sender delay interval is the amount of time before each multicast transmission begins. A period of delay before the actual multicast transmission begins is required to allow content metadata time to propagate to the receiver SEs. Metadata contains the content file and configuration information that is necessary for the successful transmission of content files. The default sender delay interval is 16 minutes. The **multicast sender-delay** command is used to configure the duration of the delay.

When configuring the sender delay interval, you must take into account that the content metadata must first be propagated to the receiver before the multicast transmission can commence. During a multicast session, a receiver SE sends out periodic requests for files that it has not yet received. The sender retransmits files only as requested by the receiver SE. A multicast receiver rejects a multicast sender's advertisement of a file if the associated content metadata has not arrived yet. The sender delay option allows you to configure enough time for the metadata to propagate to the receiver and avoid having the receiver reject the multicast sender's advertisement of a file.



**Note** The sender delay interval cannot be configured using the CDSM.

## Assigning Multicast Clouds to Delivery Services

Before you can assign a Multicast Cloud to a Delivery Service, the Delivery Service must be multicast-enabled. One Multicast Cloud can be used in multiple Delivery Services, the **IP address to use for this Delivery Service** is just different for each Delivery Service.



**Note** When a Multicast Cloud is assigned to a Delivery Service, the SEs that are part of the Multicast Cloud must also be individually assigned to the Delivery Service for multicasting. Assign the Multicast Cloud to the Delivery Service first, then assign the individual SEs to the Delivery Service.

To enable a Delivery Service for multicast and assign a Multicast Cloud to the Delivery Service, follow these steps:

- Step 1** Choose **Services > Service Definition > Delivery Services > Definition**. The Delivery Service definition page is displayed.
- Step 2** Enable multicasting on the Delivery Service. From the **Unicast Multicast Option** field, click either **Multicast only** radio button or **Multicast Unicast** radio button.
- Step 3** Click **Submit**.
- Step 4** From the left-panel menu, choose **Assign Multicast Cloud**. The Multicast Cloud table is displayed.
- Step 5** Click the **Assign** icon in the task bar. The Assign Multicast Cloud page is displayed.
- Multicast clouds must first be defined before they can be added to a multicast-enabled Delivery Service. See the “[Creating Multicast Clouds](#)” section on page 5-8 for more information.
- Step 6** From the **Multicast Cloud** drop-down list, choose a Multicast Cloud. The page refreshes, showing the IP address range for that Multicast Cloud and the automatically selected IP address for this Delivery Service.
- Step 7** In the **IP address to use for this Delivery Service** field, if the automatically selected IP address is not acceptable, enter any available IP address from the IP multicast address range.
- Step 8** In the **Carousel Pass for this Delivery Service** field, enter a value greater than 0 and less than or equal to **# of Carousel passes** configured at “[Creating Multicast Clouds](#)” section on page 5-8. The default value is **# of Carousel passes** configured at the Global Multicast Cloud.
- Step 9** From the **FEC Transmission Group** drop-down list, set the value to the FEC Transmission Group configured at “[Creating Multicast Clouds](#)” section on page 5-8. The default value is **FEC Transmission Group** configured at the Global Multicast Cloud.



**Note** We recommend that you use the default value for optimum performance.

- Step 10** In the **Max Data Rate Bandwidth for this Delivery Service** field, enter a value less than or equal to Default Multicast-out Bandwidth configured at “[Creating Multicast Clouds](#)” section on page 5-8.
- Step 11** In the **Max Concurrent Sessions for this Delivery Service** field, set the value less than or equal to Max Concurrent Sessions configured at “[Creating Multicast Clouds](#)” section on page 5-8.
- Step 12** Uncheck the **Enable check point transfer for this Delivery Service** check box, to configure the FEC proactive parity delay for this Delivery Service. The **Enable check point transfer for this Delivery Service** check box is checked by default.
- Step 13** In the **FEC proactive parity size for this Delivery Service** field, enter a value lesser than the **FEC Transmission Group**.
- Step 14** The **FEC proactive parity delay for this Delivery Service** field value is represented in milliseconds.
- Step 15** Click **Submit** to save the settings.

---

To remove a Multicast Cloud from a Delivery Service, click the **Edit** icon next to the Multicast Cloud that you want to remove. The assigned Multicast Cloud page is displayed. Click the **Trash** icon in the task bar.

## Creating Storage Priority Classes

Assigning a cache storage priority to a Delivery Service enables the CDN operator with multiple tenants to provide preference settings for keeping cached content for a Delivery Service. By default, the Content Manager deletes cached content based on popularity (an algorithm involving the number of cache hits, the size of the content object, and the decay of the content object). The cache storage priority setting assigned to a Delivery Service influences the content popularity and thereby the content that is evicted.

Each cache storage priority class is identified with a name and has a popularity multiplication factor. The popularity multiplication factor ranges from 0 to 100, where 0 is the lowest priority and 100 is the highest priority. If no cache storage priority classes are defined or assigned to a Delivery Service, the default multiplication factor of 50 is used.

Following are two examples of how the storage priority class is applied:

- Content with a storage priority class of 100 that is accessed once has the same priority as content with a storage priority class of 50 that is accessed twice.
- Content with a storage priority class of 0 is always the first to be evicted regardless of how many times the content is accessed.

The storage priority class must first be defined before it can be assigned to a Delivery Service. To define a storage priority class and assign it to a Delivery Service, follow these steps:

- 
- Step 1** Choose **Services > Service Definition > Storage Priority Classes**. The Storage Priority Classes Table is displayed.
- Step 2** In the task bar, click the **Create New** icon. The Storage Priority Class Definition page is displayed. To edit a storage priority class, click the **Edit** icon next to the storage priority class name.
- Step 3** Enter the settings as appropriate. See [Table 5-6](#) for descriptions of the fields.

**Table 5-6 Storage Priority Class Definition Fields**

Field	Description
Class Name	Unique name for the storage priority class.
Storage Popularity Multiplication Factor	Factor used to multiply the popularity of the content by. The range is from 0 to 100, where 0 is the lowest priority and 100 is the highest priority. Content with a Storage Popularity Multiplication Factor of 0 is always evicted first, regardless of popularity calculated. The default is 50.
Comments	Information about the storage priority class.

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

After creating a storage priority class, you can assign it to a Delivery Service. See the “[Service Definition](#)” section on page 5-17.

If the multiplication factor of a priority class is modified, or the Delivery Service priority class assignment changed, the change is only applied to new accesses to the content, none of the existing popularity calculations are affected. The storage priority class multiplication factor corresponding to the content is used with each access from the protocol engine. Each access is multiplied with the multiplication factor when updating the popularity.

A priority class definition cannot be deleted if it is assigned to a Delivery Service. To delete a priority class, first unassign it from all delivery services by changing the setting of the **Storage Priority Class**, then delete the priority class.

## Creating Delivery Service

A Delivery Service is a configuration used to define how content is acquired, distributed, and stored in advance of a client request. For more information about delivery services, see the “[Delivery Service](#)” section on page 2-3.

Before creating delivery services, make sure that the devices that participate in the Delivery Service are configured for the type of content to be delivered.

A Delivery Service configuration consists of the following steps:

1. [Service Definition, page 5-17](#)
2. [General Settings, page 5-21](#)
3. [Authorization Plugins, page 5-27](#)
4. [Assign Multicast Cloud, page 5-29](#)
5. [SE and Content Acquirer Assignment or Device Group and Content Acquirer Assignment, page 5-29](#)
6. [Assign IP address, page 5-31](#)
7. [Location Settings, page 5-32](#)
8. [Service Engine Settings, page 5-32](#)
9. [Identifying Content, page 5-33](#)

Configuration steps 1 through 5 are described in the following procedure. Identifying content is described in the “[Identifying Content](#)” section on page 5-33.



- Tip** For information about verifying a Delivery Service, see [Appendix J, “Verifying the Videoscape Distribution Suite, Internet Streamer.”](#)

To create a Delivery Service, follow these steps:

#### 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 5-4](#)).

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

**Figure 5-4** Delivery Service Definition Page

**Delivery Service Information**

Name:

Service Routing Domain Name:

Origin Server:

Content origin:

Live Delivery Service:

Preposition Storage Quota: 0 MB

Session Quota: 0

Session Quota Augment Buffer: 10 % (0-1000)

Bandwidth Quota: 0 Kbps

Bandwidth Quota Augment Buffer: 10 % (0-1000)

Storage Priority Class: default

**Acquisition and Distribution Properties**

Distribution Priority: Medium  Use null cipher for Distribution:

Unicast Multicast Option:  Unicast only  Multicast only  Multicast Unicast

Content Acquirer failover/fallback grace period: 120 mins Never  If there is only one SE in root location or if 'Never' is selected, failover/fallback will not occur.

Use system-wide settings for QoS for unicast data:  System-wide QoS settings page is under the Systems Tab.

QoS value for unicast data: Default or  Select DSCP from the drop-down or enter decimal value in the text field.

QoS value for multicast data: Default or  Select DSCP from the drop-down or enter decimal value in the text field.

QoS value for content ingest: Default or  Select DSCP from the drop-down or enter decimal value in the text field.

QoS value for content delivery: Default or  Select DSCP from the drop-down or enter decimal value in the text field.

**Comments**

Note: \* - Required Field

**Step 3** Enter the settings as appropriate. See [Table 5-7](#) for a description of the fields.

**Table 5-7** Delivery Service Definition Fields

Field	Description
<b>Delivery Service Information</b>	
Name	Unique name for the Delivery Service created for each content origin. <b>Note</b> Spaces are not allowed in the Delivery Service name. Multiple delivery services with same name can be created for different content origins.
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, see the “Content Origins” section on page 5-1.

**Table 5-7** *Delivery Service Definition Fields (continued)*

Field	Description
Live Delivery Service	<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 the fields in the Acquisition and Distribution Properties area.</p>
Preposition Storage Quota	<p>Maximum content disk storage size for each SE, in megabytes, for prefetched content and metadata, and hybrid metadata for this Delivery Service.</p> <p><b>Note</b> The Preposition Storage Quota configured does not affect cache content quota size; it only restricts prefetched content storage for each SE. If the total prefetched content storage size is less than the configured quota, then the extra storage is used for dynamic cache files.</p>
Session Quota	<p>Maximum number of concurrent sessions allowed for this Delivery Service. The default is zero, which means no session limits are set for this Delivery Service.</p> <p>For more information, see the “Wholesale CDN” section on page 2-30.</p>
Session Quota Augment Buffer	<p>Buffer, as a percentage, of the maximum number of concurrent sessions allowed over the Session Quota. If this threshold is exceeded, no new sessions are created until the number of concurrent sessions is below this threshold. The range is from 0 to 1000. The default is 10.</p> <p>For more information, see the “Wholesale CDN” section on page 2-30.</p>
Bandwidth Quota	<p>Maximum bandwidth allowed for this Delivery Service. The default is zero, which means no bandwidth limits are set for this Delivery Service.</p> <p>For more information, see the “Wholesale CDN” section on page 2-30.</p>
Bandwidth Quota Augment Buffer	<p>Buffer, as a percentage, of the maximum bandwidth allowed over the Bandwidth Quota. If this threshold is exceeded, no new sessions are created until the bandwidth used is below this threshold. The range is from 0 to 1000. The default is 10. For more information, see the “Wholesale CDN” section on page 2-30.</p>
Storage Priority Class	<p>Select the storage priority class to assign to the Delivery Service. For more information, see the “Creating Storage Priority Classes” section on page 5-15.</p>

**Table 5-7** Delivery Service Definition Fields (continued)

Field	Description
<b>Acquisition and Distribution Properties</b>	
Distribution Priority	<p>Content distribution priority setting. Options are High, Medium, and Low. The default is Medium.</p> <p><b>Note</b> 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> <p><b>Note</b> When a Delivery Service is configured for multicast distribution sometimes, a file from high priority Delivery Service may be scheduled after the files from lower priority Delivery Service are scheduled. This occurs when the files are placed in the time lane queue in the order of the time they were processed (FIFO). Only when the files are placed in priority queue, they are scheduled based on the decreasing order of the priority.(Highest priority deliver service file are scheduled first) The scheduling of the files between the priority lane and time lane depends on the algorithm that considers the bandwidth available in the lane and the percentage weight-age calculation for the priority lane. The files that are available for scheduling depends on when they were acquired completely and are ready for multicast sending.</p>
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 “Content Acquirer Redundancy” section on page 1-52.
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><b>Note</b> If an SE is configured with the <b>ip dscp all</b> command, this setting overrides both the system-wide QoS setting and any Delivery Service QoS setting.</p>
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> <p><b>Note</b> If an SE is configured with the <b>ip dscp all</b> command, this setting overrides both the system-wide QoS setting and any Delivery Service QoS setting.</p>

**Table 5-7** *Delivery Service Definition Fields (continued)*

Field	Description
QoS value for multicast data	<p>Configures a Differentiated Services Code Point (DSCP) value for the QoS. The multicast data refers to the distribution traffic among SEs and NAK messages sent by the Streamers to Content Acquirer for missed packets.</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> <p><b>Note</b> If an SE is configured with the <b>ip dscp all</b> command, this setting overrides both the system-wide QoS setting and any Delivery Service QoS setting.</p>
QoS value for content ingest	<p>Configures a Differentiated Services Code Point (DSCP) value for the QoS. Content Ingest refers to the ingest traffic from Content Acquirer and Web Engine to the Origin Server.</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> <p><b>Note</b> If an SE is configured with the <b>ip dscp all</b> command, this setting overrides both the system-wide QoS setting and any Delivery Service QoS setting.</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> <p><b>Note</b> If an SE is configured with the <b>ip dscp all</b> command, this setting overrides both the system-wide QoS setting and any Delivery Service QoS setting.</p>
Comments	Information about the Delivery Service.



**Note** The Flash Media Streaming DSCP marking is configured differently by Service Rule file.

**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 that you want to delete, and click the **Delete** icon in the task bar.

#### General Settings

**Step 5** From the left-panel menu, choose **General Settings**. The General Settings page is displayed.

**Step 6** Enter the settings as appropriate. See [Table 5-8](#) for a description of the fields.

**Table 5-8 General Settings Fields**

Field	Description
Maximum bitrate limit per session for HTTP	<p>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.</p> <p>To configure a Delivery Service for non-paced HTTP sessions, set the <b>Maximum bitrate limit per session for HTTP</b> field to 0. This setting provides best-effort behavior and sessions use the available bandwidth.</p> <p>When the content file is smaller than the chunk size, UKSE sends the entire file immediately. In this case, UKSE does not check pacing; therefore, the bit rate for files smaller than the chunk size is not honored.</p>
Disable HTTP Download	<p>Check the <b>Disable HTTP Download</b> check box to not allow clients to download HTTP content through this Delivery Service. This option disables all HTTP-based content served from this Delivery Service. The Web Engine returns a 403 forbidden message.</p> <p><b>Note</b> Because the Web Engine receives all HTTP requests before either Windows Media Streaming or Flash Media Streaming, if you disable HTTP download for a Windows Media Streaming Delivery Service or a Flash Media Streaming Delivery Service, and a client uses an HTTP request to download the SWF file, the Web Engine returns a 403 forbidden message.</p>
Enable Content Flow Trace	The Content Flow Trace and the Filter Trace Flow to Client are used for debugging purposes to monitor the path a request takes through the VDS-IS in case of errors. They should not be enabled during high traffic loads.
Enable Filter Trace Flow to Client	<p>Check the <b>Enable Content Flow Trace</b> check box to enable the content flow trace for the Delivery Service. Check the <b>Enable Filter Trace Flow to Client</b> check box to enable sending the response information as part of the HTTP headers to the client.</p> <p>For more information, see the “Content Flow Trace” section on page 8-64.</p> <p><b>Note</b> Authorization Server and Transaction Logging must be enabled on each SE in the Delivery Service for Content Flow Trace and Filter Trace Flow to Client to work properly.</p>

**Table 5-8 General Settings Fields (continued)**

Field	Description
Enable streaming over HTTP	Check the <b>Enable streaming over HTTP</b> check box and specify the file types in the <b>HTTP Allowed Extensions</b> 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 nsclog.
HTTP Allowed Extensions	If you want Windows Media Streaming to serve HTTP requests, check the <b>Enable streaming over HTTP</b> check box.
	<p><b>Note</b> The <b>Enable streaming over HTTP</b> check box should be checked if the content origin for this Delivery Service is used for a live program.</p>
	<p><b>Note</b> For MP3 live streaming (which uses the Web Engine), if a Windows Media player client requests an MP3 and the request URL does not have a file extension, and if the <b>HTTP Allowed Extensions</b> field contains “none,” then the playback fails because the Windows Media Streaming engine attempts to play the stream instead of the Web Engine. For the Delivery Service to support MP3 live streaming, either uncheck the <b>Enable streaming over HTTP</b> check box or remove “none” from the <b>HTTP Allowed Extensions</b> field. MP3 live streaming only supports the Icecast and Shoutcast origin servers. The supported mime-types (codecs) are “audio/mpeg” and “audio/aacp.”</p>
	<p>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.</p>
Enable Per URL Statistics	Check the <b>Enable Per URL Statistics</b> check box, to have the Delivery Service monitoring per Delivery Service. By default, the Delivery Service monitoring is disabled.
Outgoing Cookie	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.
Enable Error Response Caching	Check the <b>Enable Error Response Caching</b> check box and enter the error status codes (space delimited) that are able to be cached in the <b>Cacheable Error Responses</b> field.
Cacheable Error Responses	By default, the error status codes that are able to be cached (400, 403, 404, 500, and 503) are listed.
Follow Origin Server redirects	Check the <b>Follow Origin Server redirects</b> check box to have the Web Engine handle 302 redirects rather than forwarding the response to the client. If the <b>Follow Origin Server redirects</b> is not enabled, a 302 redirect sent from the Content Acquirer to the SE is sent back to the client. If the Origin server redirects the request to an external server, the client makes the connection to the external server to get the asset, which completely bypasses the VDS-IS. If the <b>Follow Origin Server redirects</b> is enabled, the destination server may return any other valid HTTP response, which may be sent back to the client.
Number of redirects allowed	<p><b>Number of redirects allowed</b> sets the number of times a redirect is followed. If the number of redirects is exceeded, an error is returned to the client. The default is 3. The range is from 1 to 3.</p>
	<p>As an example, if the <b>Number of redirects allowed</b> is set to 2 and the Origin server redirects to a server B, B redirects to C, and C redirects to D, then only redirection to C is followed. When C returns 302, the Web Engine on the SE returns an error code 310 to the client.</p>
	<p><b>Note</b> The Follow Origin Server Redirect feature is not supported for the HEAD request; only the GET request is supported.</p>

**Table 5-8 General Settings Fields (continued)**

Field	Description
URL Hash Level for Cache Routing	<p>Enter the directory level that is used to calculate the URL hash for cache routing. The range is from 0 to 10. The default, 0, means use the entire URL to create the hash.</p> <p>The URL hash is used by the Cache Router in selecting an upstream SE. The URL hash calculation is based on the directory level. By setting the <b>URL Hash Level for Cache Routing</b> to a directory level of a URL, all URLs that have the same directory structure take the same hierarchical path to the origin server.</p> <p>For example, if the <b>URL Hash Level for Cache Routing</b> field is set to 5, then all content URLs that have the same directory structure up to the fifth directory level are routed the same. For this example, the portion of the URL in bold is the included directory level:</p> <p><code>http://ofqdn/content/<b>content_type</b>/moviename/<b>quality</b>/filename</code></p> <p><b>Note</b> If the upstream SE has reached a threshold causing the liveness query to fail, the request goes to the parent SE. As long as the threshold have not been exceeded, all URLs with the same directory level take the same path for the configured directory level.</p>
HTTP Response Read Timeout	<p>If the Origin server does not respond within the <b>HTTP Response Read Timeout</b>, the connection is terminated and the content is not served. Similarly, if the upstream SE does not respond within the <b>HTTP Response Read Timeout</b>, the connection is not terminated immediately, and this request will continue to next Upstream SE, till CA, If the CA still does not respond within timeout, this request is forwarded to Original Server. The default is 5. The range is from 1 to 60.</p> <p><b>Note</b> If the Follow Origin Server Redirect feature is enabled, the <b>HTTP Response Read Timeout</b> value is used for each redirected Origin server. Because each Origin server may have a different idle period, it may cause additional delays to the user depending on the value and frequency of the idle periods.</p>
Disable Dynamic Caching	<p>Check the <b>Disable Dynamic Caching</b> check box to disable dynamic caching. By default, dynamic caching is enabled. See the “<a href="#">Dynamic Caching</a>” section on page 1-20 for more information.</p> <p><b>Note</b> The cache revalidation of the content is not be done if dynamic caching is disabled. The Service Engine will serve client requests for which it finds a prepositioned content or cached content available before the dynamic caching was disabled. Any invalid cached data is served to the client even though the content is changed in the Origin Server.</p>

**Table 5-8 General Settings Fields (continued)**

Field	Description
Disable File Caching on Disk	Check the <b>Disable File Caching on Disk</b> check box to not cache any content on disk.
Memory Cache Duration	<p>The small files are cached in tmpfs and stay in the tmpfs for a period of time that is configured in <b>Memory Cache Duration time</b>. An internal Web Engine timer is triggered every 4 seconds. If the cache duration for a small file is complete and its corresponding DataSource is not serving a client, the file in tmpfs is deleted.</p> <p> <b>Caution</b> Sometimes, the file in tmpfs may be early evicted before its cache duration is complete. For example, running out of tmpfs space, or running out of file descriptors, or there are too many active DataSources.</p>
	<p><b>Memory Cache Duration</b> field is configured with an integer value when the <b>Disable File Caching on Disk</b> is checked. The range is 4 to 60 seconds. The default value is 4 seconds.</p>
	<p><b>Note</b> The Memory Cache Duration is selected carefully to prevent excess memory usage for Web Engine. If the cache duration is large, more files are cached in tmpfs. Managing more number of files costs more memory usage for a Web Engine.</p>
	<p><b>Note</b> We recommend that you increase the Memory Cache Duration value only for ABR Live services.</p>
Memory Cache Size	Enter the maximum file size (in MB) that defines a small file. The range is from 1 to 10 MB. The default is 2 MB.
Origin Server HTTP Port	<p>Port used by Web Engine to communicate with Origin servers. Default is 80. Range is from 1 to 65535. Well-known port numbers are not allowed. For the list of well-known ports, see the “<a href="#">System Port Numbers</a>” section on page 8-10.</p> <p><b>Note</b> If the Origin Server HTTP Port is set to a different port than the default (80), then the port number of the Origin server must be included in the URL when adding content. See the “<a href="#">Identifying Content</a>” section on page 5-33.</p>
Skip Location Leader Selection for Edge SE	<p>When the <b>Skip Location Leader Selection for Edge SE</b> check box is checked (option is enabled), the location leader selection is skipped at the edge location, and the edge SE directly contacts the location leader of the upstream tier. None of the other edge SEs are contacted.</p> <p>When the <b>Skip Location Leader Selection for Edge SE</b> check box is unchecked (option is disabled), the location leader selection takes place at the edge tier. The edge SE may or may not directly contact the location leader of the upstream tier or the SEs in the edge tier. Contact is based on the location leader selection.</p> <p>This option is mainly used to improve the edge-tier caching efficiency to avoid content duplication at the edge-tier SEs.</p>

**Table 5-8 General Settings Fields (continued)**

Field	Description
WMT User Agent	<p>Enter the user agents for Windows Media Streaming. The <b>WMT User Agent</b> field accept comma-separated values for identifying the user agents.</p> <p><b>Note</b> The ampersand (&amp;) cannot be used when specifying a user agent.</p> <p>The following user agents are supported for Windows Media Streaming: NSPlayer, WMServer, WMPlayer, NSServer, Windows Media Player, and VLC.</p> <p>Windows Media Streaming has been enhanced to support custom user agents that are configured through the CDSM GUI. The maximum number of user agents allowed is 32. Each user-agent identifier can have a maximum of 32 characters. The following example specifies Windows Media Player, NSPlayer, and LAVF as Windows Media Streaming user agents:</p> <p>NSPlayer, LAVF, Windows-Media-Player</p> <p><b>Note</b> The Content Origin for a Delivery Service can be used for one Delivery Service and multiple live delivery services. The <b>WMT User Agent</b> field applies to all of the delivery services associated with the same Content Origin.</p>
Enable Generic Session Tracking	Enables Generic session tracking.
Enable HSS Session Tracking	Enables HSS session tracking.
Enable HLS Session Tracking	Enables HLS session tracking.
Server Header of Response	Configures the server header of HTTP/HTTPS response. The maximum length is 32 characters.
Skip Special Header Check for MP3 Live	<p>Sometimes you may want the web engine to ignore "http version"(ICY/icecast), so that the web engine can serve their mp3 live streams.</p> <p>Check the <b>Skip Special Header Check for MP3 Live</b> button, to make sure that the http response for mp3 vod contents must have content length header filed, otherwise they will be treated as mp3 live stream by mistake.</p>
<b>HTTPS Settings</b>	
Delivery streaming protocol support	<p>To enable HTTPS when streaming to clients, in the <b>Delivery streaming protocol support</b> drop-down list, choose <b>HTTPS only</b>. The default is <b>HTTP only</b>.</p> <p>For more information about HTTPS Settings and how to configure it, see the “<a href="#">HTTPS Settings</a>” section on page 2-25.</p>
Origin Server streaming protocol support	<p>To enable HTTPS for communications with the Origin server, in the <b>Origin Server streaming protocol support</b> drop-down list, choose <b>HTTPS only</b>. The default is <b>HTTP only</b>.</p> <p>For more information about HTTPS Settings and how to configure it, see the “<a href="#">HTTPS Settings</a>” section on page 2-25.</p>
Delivery Streaming Mutual Authentication	Check the <b>Delivery Streaming Mutual Authentication</b> check box, to enable delivery streaming mutual authentication for individual Delivery Service. The default is unchecked.

**Table 5-8 General Settings Fields (continued)**

Field	Description
Delivery Streaming Supported Cipher List	<p>Input the Cipher list. The default is empty.</p> <p>When the Web Engine is acting as HTTPS server, the delivery streaming supported cipher list is used to negotiate and accept HTTPS connection from client player.</p> <p><b>Note</b> When it is empty, backend will use default string.</p> <p><b>Note</b> For more details on composing the Cipher List, see <a href="#">OpenSSL Documents</a>.</p>
Origin Server Streaming Mutual Authentication	<p>Check the check box <b>Origin Server Streaming Mutual Authentication</b> to enable Origin Server Streaming Mutual Authentication for individual Delivery Service. The default is checked.</p>
Origin Streaming Supported Cipher List	<p>Input the Cypher list. The default is empty.</p> <p>When the Web Engine is acting as HTTPS server, the origin streaming supported cipher list is used to connect to the origin server.</p> <p><b>Note</b> When it is empty, backend will use default string.</p>
Force Quota Usage Reporting	Quota usage reporting is automatically sent whenever a session quota or a bandwidth quota is configured for a Delivery Service with a setting other than zero (zero means no limits are configured). To monitor the session counter and bandwidth counter when session quota and bandwidth quota are not configured, check the <b>Force Quota Usage Reporting</b> check box.

**Step 7** Click **Submit** to save the settings.

To remove the settings from the Delivery Service, click the **Remove Settings** icon in the task bar.

### Authorization Plugins

The Authorization Plugins page allows you to upload or import a Geo/IP file and assign a Service Rule file that has been registered to the VDS-IS.

A Geo/IP file is an XML file that configures the Delivery Service to allow or deny client requests based on the client's IP address or based on the client's geographic locations (country, state, city). Each SE participating in the Authorization Service must have Authorization Service enabled and the IP address and port of the Geo-Location server specified.

[Table 5-9](#) mapping between the geo-location rule tag and the geo server response fields.

**Table 5-9 Geo-Location Rule Tags**

Geo-Location Rule Tag	Quova Response Fields	Maximum Response Fields
Country	country_code, country	Country code, Country name
State	state_code, state	Region code, Region name
City	city	City name
Netspeed	N/A	Netspeed
Connection_type	connection_type	N/A
Line_speed	line_speed	N/A
Asn	asn	N/A
Carrier	carrier	N/A

**Table 5-9 Geo-Location Rule Tags**

<b>Geo-Location Rule Tag</b>	<b>Quova Response Fields</b>	<b>Maximum Response Fields</b>
Anonymizer_status	anonymizer_status	N/A
Field (assume name="field_ID")	The field whose tag is field_ID	The field whose ordinal number is field_ID

See the “Configuring the Authorization Service” section on page 4-28 for more information. For more information on the XML configuration file for the Geo/IP file, see Appendix D, “Creating Geo/IP Files.”

A Service Rule file is an XML configuration file that specifies Service Rules for all of the SEs in the Delivery Service. For more information on the XML file for the Service Rule, see Appendix E, “Creating Service Rule Files.”



**Note** The Service Rule file is only supported for the Web Engine and Flash Media Streaming; for Windows Media Streaming and Movie Streamer, use the per-device Service Rule configuration. For more information, see the “Configuring Service Rules” section on page 4-21. The Authorization Service must be enabled on all SEs participating in a Delivery Service that uses the Service Rule file. The Authorization Service is enabled by default. For more information, see the “Configuring the Authorization Service” section on page 4-28.

**Step 8** From the left-panel menu, choose **Authorization Plugins**. The Authorization Plugins page is displayed.

**Step 9** To upload or import a Geo/IP file for the Delivery Service, follow these steps:

- In the Geo/Ip Plugin Settings area, click the **Configure** icon for Geo/Ip File. The File Management page is displayed.
- Choose a file import method from the **File Import Method** drop-down list:
  - Upload—Uploads a file from any location that is accessible from your PC using the browse feature.
  - Import—Imports a file from an external HTTP, HTTPS, or FTP server.
- Enter the fields as appropriate. Table 5-10 describes the upload method fields. Table 5-11 describes the import field methods.

**Table 5-10 Upload Method**

<b>Property</b>	<b>Description</b>
Source File Upload	Local directory path to the file. To locate the file, use the <b>Browse</b> button. Click <b>Validate</b> to validate the XML file.
Destination Filename	Name of the file. This field is filled in automatically with the filename from the local directory path.

**Table 5-11 Import Method**

<b>Property</b>	<b>Description</b>
File URL	The URL where the file is located, including path and filename. Click <b>Validate</b> to validate the XML file.
Destination File Name	Name of the file.
Update Interval	Frequency with which the CDSM looks for changes to the file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the file.
Password	User password for fetching the file.

- d. To save the settings, click **Submit**.

**Step 10** To assign a Service Rule file, follow these steps:

- a. From the **Service Rule File** drop-down list, choose a Service Rule configuration file.

The **Service Rule File** drop-down list is populated with the Service Rule files that are registered to the CDSM. See the “[Authorization File Registration](#)” section on page 6-15 for information on registering a Service Rule file.

See [Appendix E, “Creating Service Rule Files.”](#) for information on creating a Service Rule file.

- b. Click **Submit**.

### Assign Multicast Cloud

See the “[Assigning Multicast Clouds to Delivery Services](#)” section on page 5-14 for information on assigning multicast clouds to a Delivery Service.



The Multicast Cloud feature is supported in all releases starting with Release 3.1.1.

### SE and Content Acquirer Assignment or Device Group and Content Acquirer Assignment

[Step 11](#) through [Step 14](#) 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 11](#) through [Step 14](#) 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 11** From the left-panel menu, choose **Assign Service Engines**. The Service Engine Assignment page is displayed ([Figure 5-5](#)).

**Figure 5-5 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

Submit Cancel 209842

- Step 12** Click the **Assign** icon (blue cross mark) next to the SE that 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 5-6.

**Figure 5-6 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 cross mark indicates that an SE assignment is ready to be submitted. To unassign an SE, click this icon.

- Step 13** 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 5-54.

- Step 14** 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.



**Note** When devices are unassigned from a Delivery Service sometimes the contents are not cleaned up. **cdnfs cleanup** CLI command is used to remove the stale contents.



To view all of the Service Engines assigned to the Delivery Service, in the left-panel menu, click **Service Engine Settings**.

### Assign IP address

The Multiple Logical IP addresses feature allows the configuration of multiple logical IP addresses for each Gigabit Ethernet interface, port channel, or standby interface on an SE. Each logical IP address can be assigned to a Delivery Service. The same logical IP address can be used for more than one Delivery Service as long as the delivery services use the same content origin.

These new configured secondary ip addresses should be in the show running-config output command, and the configuration should be restored after reload.


**Note**

Starting with Release 3.3, VDS-IS supports assigning multiple IP addressing different subnets on a port channel. For more information on the new CLI commands, see the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference Guide*.

The Multiple Logical IP addresses feature supports up to 24 unique IP addresses within the same subnet for the same interface. The netmask is unique per interface, which means for a single interface you cannot have multiple IP addresses with different netmask values. Up to 24 unique IP addresses are supported in the SE to SR keepalive messages.

To configure multiple IP addresses on an interface use the **IP address** command multiple times in the config-if mode, or use the range keyword option (**IP address range**).

```
(config-if)# IP address <ip_addr> <subnetmask>
(config-if)# IP address range <lower_ip_addr_range> <upper_ip_addr_range> <subnetmask>
```

To view configured IP address for an interface, use the **show interface** command or the **show running-config** command. The IP address assignments for each SE can also be displayed in the CDSM GUI by viewing the Network Interfaces page (**Devices > Devices > General Settings > Network > Network Interfaces**).


**Note**

The SNMP trap operations are performed per interface and not per IP address. However, transaction logs include the server IP address.

If a Delivery Service is mapped to a specific IP address, the SR does not perform load balancing to any other IP address. If the Delivery Service is not mapped to an IP address, load balancing is performed.

The CLI is used to assign the multiple IP addresses to each interface on the SE. For information on the **interface** command, see the *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference*.

The IP address assignments for each SE can be displayed in the CDSM GUI by viewing the Network Interfaces page (**Devices > Devices > General Settings > Network > Network Interfaces**).


**Note**

Removing an IP address from a Delivery Service interrupts the service. Changing an IP address for a Delivery Service causes all new requests to use the new IP address.

If you use Device Groups for delivery services, assigning IP addresses to the SE interfaces must happen before assigning the device to the device group.

**Step 15** To assign an IP address of an SE to a Delivery Service, click **Assign IP address** from the left-panel menu. The Interface IP Entries page displays the SEs assigned to this Delivery Service.

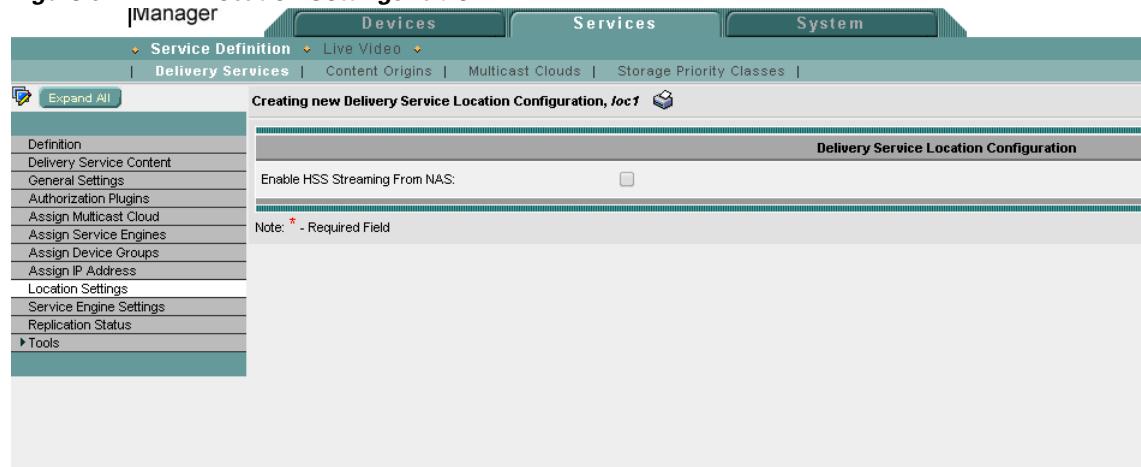
**Step 16** Click the **Edit** icon next to the SE you want to assign the IP address. The Modify IP Assignment page is displayed.

- Step 17** In the **Address** field, enter the IP address for the SE.
- Step 18** In the **Ipv6 Address** field, enter the IPv6 address for the SE.
- If the dual-stack client intent is to use either (IPv4 or IPv6) transports, map both the IPv4 address and IPv6 address of the Service Engine to the Delivery Service.
- Step 19** Click **Submit**.

### Location Settings

- Step 20** To enable HSS Steaming from NAS, click **Location Settings** from the left-panel menu. The Location Settings table is displayed (Figure 5-7).

**Figure 5-7 Location Settings Table**



The Location Settings table lists the locations for the SEs associated with the Delivery Service. For more information about locations, see the “[Configuring Locations](#)” section on page 4-1.

To track ABR and Generic sessions using transaction logs for the custom-format Web Engine transaction logs and the Per Session log, the Generic Session Tracking, the HLS Session Tracking and HSS Session Tracking must be enabled for the SEs in all locations of each Delivery Service. For more information about ABR Session Tracking and Generic Session Tracking, see the “[Web Engine User Level Session Transaction Logs](#)” section on page 8-96.

- Step 21** Enter the settings as appropriate. See [Table 5-12](#) for a description of the fields.

**Table 5-12 Location Settings Fields**

Field	Description
Enable HSS Streaming from NAS	Enables HSS from Network-attached Storage (NAS) devices. <b>Note</b> Not supported.



**Note** The URL Resolve Rule does not work when ABR Session Tracking is enabled.

### Service Engine Settings

The Service Engine Settings page displays a list of all service engines, and allows you to configure the delivery setting for a specific SE. If the general settings are available for the Delivery Service, then, by default, the SE is configured with the general settings.

**Step 22** Click the **Edit** icon next to the SE that you want to change the settings. The Creating new SE Settings page is displayed.

**Step 23** Check the **Disable File Caching on Disk** check box to not cache any content.

**Memory Cache Duration** field is configured with an integer value when the **Disable File Caching on Disk** is checked. The range is 4 to 60 seconds. The default value is 4 seconds.

**Step 24** Click **Submit**.

## 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 that you have already defined the Delivery Service (see the “[Creating Delivery Service](#)” section on [page 5-16](#)).



**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 5-47](#).

## Identifying Content Using the CDSM

There are several options in 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 5-13 describes the icons for identifying content using the CDSM.

**Table 5-13 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 view (-) 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 2-10.

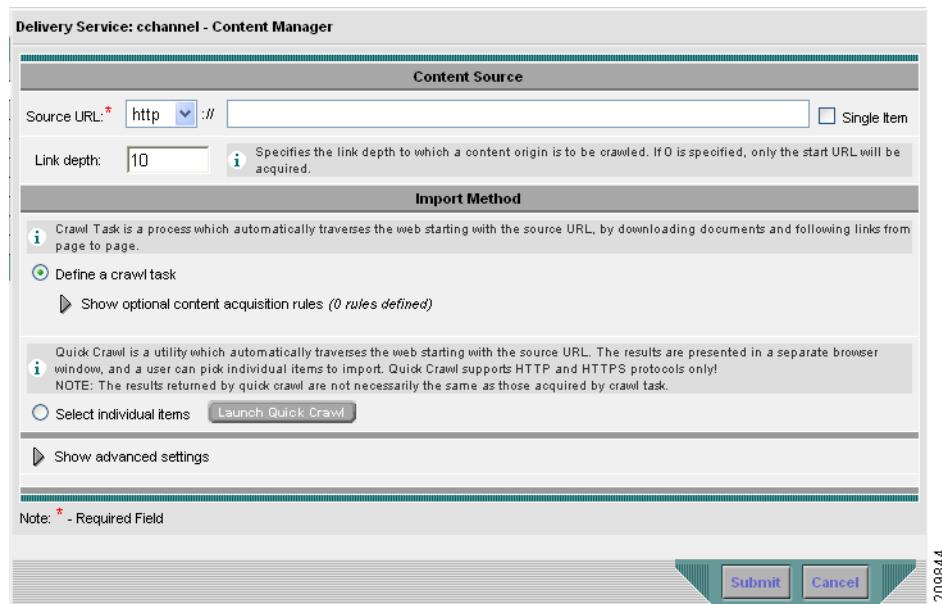
To identify content for acquisition using the CDSM, follow these steps:

- 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 5-8](#)).

**Figure 5-8 Content Table Page**

The screenshot shows a table titled "Content Items" with columns: URL, Type, Start, Stop, and Depth. The table contains three rows, each representing a content item with a checkbox, a small icon, and the URL "http://171.71.50.61/16B.html". The "Type" column shows "Item" for all three rows. The "Start" and "Stop" columns are empty. The "Depth" column is also empty. At the bottom of the table, it says "Showing 1-3 of 3 Content Items". Below the table, there are buttons for "All", "None", and "Edit Selected Items".

- Step 2** Click the Add Content icon in the task bar. The Content Manager page is displayed ([Figure 5-9](#)).

**Figure 5-9 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 5-42](#).

**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. If the **Origin Server HTTP Port** in the **Delivery Services > General Settings** page is set to a different port than the default (80), then the port number of the Origin server must be included in the URL when adding content.



**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 see the “[Configuring Advanced Settings](#)” section on [page 5-39](#) 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 see the “[Defining a Crawl Task](#)” section on [page 5-36](#) 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 see “[Launching Quick Crawl](#)” section on [page 5-37](#) 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.

## Configuring Delivery Services

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.

## Defining a Crawl Task

To define a crawl task, follow these steps:

**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 re-parsed, changes are detected, and the corresponding content items are acquired or removed.
- Go to the “[Configuring Advanced Settings](#)” section on page 5-39, 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 5-10](#)), and the arrow becomes the **Hide Optional Content Acquisition Rules** arrow.

**Figure 5-10 Content Manager Page—Acquisition Rules Fields**

MIME Type	Extension	Time Before	Time After	Min Size	Max Size
video/mpeg	mpg	10/21/2006 00:00:00	10/21/2007 00:00:00		

Quick Crawl is a utility which automatically traverses the web starting with the source URL. The results are presented in a separate browser window, and a user can pick individual items to import. Quick Crawl supports HTTP and HTTPS protocols only!

NOTE: The results returned by quick crawl are not necessarily the same as those acquired by crawl task.

**Step 4** Enter the settings as appropriate. See [Table 5-14](#) for a description of the fields.

**Table 5-14 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). <b>Note</b> The MIME type cannot exceed 32 characters.
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 TZM (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 TZM (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 area to save the edits.

To delete a content acquisition rule, click the **Edit** icon next to the rule. Click **Delete** in the content acquisition rules area. 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:

- a. If this is a new crawl task, click **Submit**.
- b. If you are editing an existing crawl task, click **Update**.
- c. Go to the “Configuring Advanced Settings” section on page 5-39, 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, follow these steps:

- 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 5-15](#) for a description of the fields.

**Table 5-15 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.  If entered, the value from the Content Manager page is brought over to this field.
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 that 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 of 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, follow these steps:

- Step 1** Click the **Show Advanced Settings** arrow. The Advanced Settings fields are displayed (Figure 5-11), and the arrow becomes the **Hide Advanced Settings** arrow.

**Figure 5-11 Content Manager Page—Advanced Settings Fields**

The screenshot shows the 'Content Manager' page under 'Delivery Service: cchannel - Content Manager'. The 'Show Advanced Settings' arrow is expanded, revealing several sections of configuration fields:

- Content Serving Time:** Includes 'High priority content' checkbox, 'Start serving time' and 'Stop serving time' date/time pickers, and UTC checkboxes.
- Authentication:** Includes 'Use weak SSL certificate' checkbox, 'Disable basic authentication' checkbox, 'Windows Media Playback Authentication' dropdown ('As acquired'), and user credentials fields for 'User name' and 'Password'.
- URL Settings:** Includes 'Ignore query string' checkbox.
- Content Settings:** Includes 'TTL' and 'Retry interval' fields, both with 'Minutes' dropdowns and explanatory text about re-checking frequency.

At the bottom, there is a note: "Note: \* - Required Field". The footer includes 'Submit' and 'Cancel' buttons, a timestamp '209846', and a page number '209846'.

- Step 2** Enter the settings as appropriate. See Table 5-16 for a description of the fields.

**Table 5-16 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	<p>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>.</p> <p>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.</p>
Stop Serving Time	<p>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>.</p> <p>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="#">Delivery Services Table</a>” section on page 8-30.</p>
<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	<p>Sets the authentication for Windows Media playback to one of the following:</p> <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.

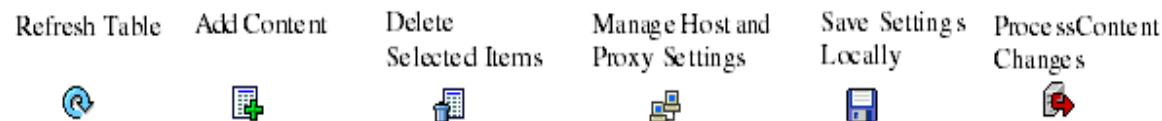
**Table 5-16 Advanced Settings for Serving Content (continued)**

Field	Description
<b>Content Settings</b>	
TTL	<p>Time period for revalidation of content. Select unit of measure from the drop-down list.</p> <p>If no TTL is entered, the content is fetched only once, and its freshness is never checked again.</p> <p><b>Note</b> Revalidation is enabled by default for the Web Engine.</p>
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 re-parsed, changes are detected, and the corresponding items are acquired or removed. This action, however, does not trigger a recheck of all of the content in the Delivery Service.
- 

## Content Table

The Content Table page ([Figure 5-13](#)) offers the task bar functions described in [Figure 5-12](#).

**Figure 5-12 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 that 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 5-13 Content Table Page**

URL	Type	Start	Stop	Depth
http://171.71.50.61/16B.html	Item			
http://171.71.50.61/4GB_1100kbs.wmv	Item			
http://171.71.50.61/8KB.html	Item			

For information on the **Manage Host and Proxy Settings** icon, see the “[Configuring Proxy Server Settings](#)” section on page [5-42](#).

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 5-43](#) and [Appendix B, “Creating Manifest Files.”](#)

To edit multiple content items, check the check box next to each item that 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 receive the message: “failed: Connection refused.”

To configure a proxy server for content items identified using the CDSM, follow these steps:

**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 that 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 5-17](#) for a description of the fields.

**Table 5-17 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.  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.



**Note** Before configuring the CDSM to receive the Manifest file, you need to create one. See [Appendix B, “Creating Manifest Files.”](#) for details on creating a Manifest file. 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.



**Note** If a Manifest file is located on an Origin server that requires custom HTTP header authentication, fetching the Manifest file by using the **Specify external manifest file** method fails. The Manifest file must be located on a server that does not require custom HTTP header authentication.

To configure the Manifest file settings, follow these steps:

- 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, follow these steps:
- Click **Change Method**.
  - From the drop-down list, choose **Specify external manifest file**.
  - Click **Save**.
  - In the confirmation dialog box, click **OK**.

The Content Manager page displays the Manifest file settings (Figure 5-14).



**Note** When you change the Content acquisition method for Delivery Service from the content acquisition page to Specify external manifest file, 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 5-14 Content Manager Page—Manifest File Settings**

- Step 3** Enter the settings as appropriate. See [Table 5-18](#) for a description of the fields.

**Table 5-18 Manifest File Settings Fields**

Field	Description
<b>Define Basic Manifest Settings</b>	
Manifest URL	<p>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.</p> <p>To validate the Manifest file from this page, click <b>Validate</b>. A new page displays the validation results. For more information, see the “<a href="#">Manifest Validator Utility</a>” section on page <a href="#">B-15</a>.</p>
Check Manifest Every	<p>Frequency, in minutes (0 to 52560000), at which the Content Acquirer assigned to the Delivery Service checks for updates to the Manifest file.</p> <p>To fetch the Manifest file now, click <b>Fetch Manifest Now</b>.</p>
Weak Certificate Verification	<p>When checked, enables weak certificate verification for fetching the Manifest file. This is applicable when the Manifest file is fetched using HTTPS.</p> <p><b>Note</b> To use weak certification for content ingest, you need to specify weak certification within the Manifest file.</p>
Manifest Username	<p>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.</p> <p><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.</p>
Manifest Password	Password for the user.
Confirm Password	Password confirmation.
<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.
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.

**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, follow these steps:

- a. From 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” area, 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 8-37.

## 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 VDS-IS 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 Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference*. For online documentation, see the “[Related Documentation](#)” section on page [xx](#).

# Configuring Programs

A program in the VDS-IS is defined as a scheduled live or rebroadcast event that streams content to client devices. The VDS-IS 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 [2-20](#).

To view existing programs, see the “[Viewing Programs](#)” section on page [5-59](#).

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 [1-31](#).



### 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 verifying a live or rebroadcast program, see [Appendix J, “Verifying the Videoscape Distribution Suite, Internet Streamer.”](#)

**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, follow these steps:

- 
- 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.  
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** Check the **Block per Schedule** check box if you want the live program to stop all active streams when the scheduled playtime ends.
  - Step 7** In the **Description** field, enter information about the program.
  - Step 8** Click **Submit** to save the settings.
- 

You have defined the type of program that you want to configure. Proceed to the appropriate section for configuring that type of program:

- To configure Movie Streamer live and Windows Media live programs, see [Configuring Live Programs, page 5-49](#).

- To configure Windows Media rebroadcast and Movie Streamer rebroadcast programs, see the “[Configuring a Rebroadcast](#)” section on page 5-55.

For information about copying a program, see the “[Copying a Program](#)” section on page 5-62.

## 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 5-48).

To configure a Movie Streamer live or Windows Media live program, follow these steps:

---

**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 of 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 5-16 for more information.

**Step 2** Click the radio button next to the name of the live Delivery Service that 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 5-15](#)).

**Figure 5-15 Service Engine Assignment Page**

Service Engine assignments for Delivery Service, cchannel with Quota 100000 MB						
Service Engines	Unreserved Content Cache (MB)	Total Content Cache (MB)	Status	Location	Primed	Rows: ALL
✗ NE-612-12	139942	139942	Online	NE-612-12-location	<input type="checkbox"/>	
✗ NE-612-5	119457	119457	Online	tier-1	<input type="checkbox"/>	
✗ NE-612-6	119492	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

Submit Cancel 209848

- Step 4** Click the **Assign** icon (blue cross mark) next to the SE that 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 5-16](#).

**Figure 5-16 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 cross mark 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 that you want to prime with the live stream. For more information about priming, see the “[Priming a Live Delivery Service](#)” section on page 5-54.

- 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** From 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 5-19](#) for a description of the Windows Media Live Stream Settings fields, and [Table 5-20](#) 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 5-19 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_WMSreamerServer:port/path/file (Multicast operating system)</li> <li>• rtsp://WMencoder_or_WMSreamerServer:port/path/file (Unicast operating system)</li> </ul> <p>For encoder failover, you can specify more than one encoder. Separate live source URLs in the list by using a semicolon (;).</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> <p><b>Note</b> If the Live Source URL is changed, the existing session continues to use the old URL and does not move to the new one.</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.
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	<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. 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 5-20 Movie Streamer Live Stream Settings Fields**

Field	Description
Origin Server SDP File URL	The URL for the Session Description Protocol (SDP) file generated on the encoder. From the drop-down list, choose 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.  When you click <b>Auto Populate</b> , the Incoming Live Streams Settings fields (in the Live Streaming Settings page) are automatically populated based on the Origin Server SDP File URL.
Backup SDP URL	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 (in the Live Streaming Settings page) are automatically populated based on the Backup SDP URL.  The Cisco VDS-IS 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.  When you click <b>Auto Populate</b> , the Incoming Live Streams Settings fields (in the Live Streaming Settings page) are automatically populated based on the Backup SDP URL.
<b>Incoming Live Streams Settings</b>	
<b>Note</b>	Manually enter these fields, if Auto Populate cannot populate it based on the backup SDP URL.
Source Server	The stream source IP address.
Backup Source Server	The backup stream source IP address.
Receiving IP	For RTSP, the Primary Receiving IP is the IP address of the Content Acquirer acting as the primary receiver. This is always unicast-in.  For HTTP, the Primary Receiving IP is the multicast-in IP address used to broadcast the live stream.
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.  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.

**Table 5-20 Movie Streamer Live Stream Settings Fields (continued)**

Field	Description
Enable Multicast Delivery to Client	If enabled, the program uses multicast transmission. 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: <code>http://sourceHost_or_FQDN/path/filename.sdp</code> 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. 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 5-21](#) for a description of the fields.

**Table 5-21 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. From the drop-down list, choose minutes, hours, or days as the unit of time.

**Table 5-21 Playtime Fields (continued)**

Field	Description
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 Repeat Until	These fields display when <b>Repeat Every</b> or <b>Repeat Weekly</b> are chosen for Repeat Frequency.  Repeat Forever repeats the program forever using the repeat frequency set in the previous fields.  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.

## Windows Media Streaming Live Streaming Encoder Failover

In normal situations, when a new client request is received (or priming live program is enabled) the Content Acquirer ingests the content from first encoder in the configured list (for example, rtsp://Encoder\_1:port/path/file; rtsp://Encoder\_2:port/path/file).

If the first encoder is unreachable, the Content Acquirer considers it has failed and does not attempt to contact it until the timeout period of 300 seconds has expired. The Content Acquirer attempts a connection with the failed encoder every 300 seconds.

The Content Acquirer selects a source encoder in the following way:

1. If there is an existing session that is using an encoder, then select it as the source; otherwise, select the first one in the configured list of encoders for the requested URL. If the first encoder does not have the requested URL, try the next one in the list, until an encoder with the requested URL is contacted.
  - a. If the first encoder is unreachable, try the next encoder in the list, and mark the first encoder as bad and start the timeout interval for it.
  - b. If the encoder is not marked as bad, then check to see if the encoder has the content with the requested URL.
  - c. If the encoder is marked as bad and the timeout interval has been reached, try the encoder. If the timeout interval has not been reached, check the next encoder.
2. If all of the sources are marked bad and all timeout intervals have not been reached, try the encoder that is closest to reaching the timeout interval.



**Note** An alarm is raised when an encoder is requested but cannot be reached.

The Content Acquirer supports fail over for several encoders in the following ways:

- If failure occurs during streaming a session, the streaming stops and the Windows Media Player sends another request. The reachable-encoder selection process is started as described above. The streaming session recovers automatically. The user typically only experiences around a 60-second freeze for RTSP URL content.
- “The Content Acquirer continues to ingest from the reachable encoder, even if the failed encoder recovers, for the previous streaming sessions and new incoming client requests. This provides a better end-user experience.



Alarms from Content Acquirer are cleared when the specific encoder is reachable again, or when the alarm is manually cleared through the CLI or the CDSM GUI.

## 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 5-48).



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, follow these steps:

- 
- 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 that 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 that 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** Multiple media files can be selected for Movie Streamer rebroadcasts. Playlist content is seamlessly updated without impacting current rebroadcasting.

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.



**Note** SEs must have the same NTP time. Multiple SEs can be assigned for additional redundancy, but all SEs assigned must be in different multicast domains, because all assigned SEs send packets to the same specified multicast address.

- Step 8** Click the **Assign** icon (blue cross mark) 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 5-17](#).

**Figure 5-17 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 cross mark 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 5-22](#) for a description of the Windows Media Rebroadcast Stream Settings fields, and [Table 5-23](#) for a description of the Movie Streamer Rebroadcast Stream Settings fields.

**Table 5-22 Windows Media Rebroadcast Stream Settings Fields**

Field	Description
Multicast URL Reference	The reference URL for multicast streaming has the following format: <a href="http://SRDN/program-name.nsc">http://SRDN/program-name.nsc</a> .
NSC Reference for Multicast	The URL for the NSC file used for a server-side playlist as the media source in a multicast program.
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 5-23 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 5-24](#) for a description of the fields.

**Table 5-24 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	<p>The playback options are the following:</p> <ul style="list-style-type: none"> <li>• Playback Once and Stop</li> <li>• Loop for number of minutes, hours, or days</li> </ul>

**Table 5-24 Playtime Fields (continued)**

Field	Description
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	These fields display when <b>Repeat Every</b> or <b>Repeat Weekly</b> are chosen for Repeat Frequency.
Repeat Until	Repeat Forever repeats the program forever using the repeat frequency set in the previous fields. 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 of the programs defined in your VDS-IS 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 5-48.

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 5-62 for more information.

Table 5-25 describes the icons for the Programs Table page.

**Table 5-25 Programs Table Icons**

Icon	Function
	Creates a new program. See the “Defining a Program” section on page 5-48 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 page.
	Edits a program. See the “Defining a Program” section on page 5-48 for more information.
	Previews a program.

To view all of the programs defined in your VDS-IS network, follow these steps:

- 
- Step 1** Choose **Services > Live Video > Live Programs**. The Programs Table page displays with a list of all of 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 VDS-IS network. The **All** tab displays all of the programs defined in your VDS-IS 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 5-26** describes the information that is displayed in this page.

**Table 5-26 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.

**Table 5-26 Programs Table Page Information (continued)**

Item	Description
<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. 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 re-parsing 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 5-62.)

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, follow these steps:

- 
- 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.
- You must have a Windows Media plug-in installed to view Windows Media live programs.
- You must have a 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 of 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, follow these steps:

- 
- 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 5-48.)



**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.

**■ Copying a Program**



# Configuring the System

This chapter provides information on configuring the system parameters of the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS).

- [Configuring AAA, page 6-1](#)
- [Changing a Password, page 6-7](#)
- [Configuring System Settings, page 6-8](#)
- [Viewing or Downloading XML Schema Files, page 6-24](#)

For information on logs, see the “[System Audit Logs](#)” section on page 8-9. For information on upgrading the VDS-IS software, see the “[Software Upgrade](#)” section on page 9-1. For information on the ports used by the VDS-IS, see the “[System Port Numbers](#)” section on page 8-10.

## 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, that means the information is in a single, centralized, secure database, which is much easier to administer than information distributed across numerous devices.

In the VDS-IS 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 a VDS-IS 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 describes login authentication and authorization for the CDSM. For information about device login authentication and authorization, see the “[Login Access Control](#)” section on page 4-49 and the “[Authentication](#)” section on page 4-56.

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 addresses 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:

- The 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:

- The 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, follow these steps:

- 
- Step 1** Choose **System > AAA > Users**. The User Table page is displayed.

[Table 6-1](#) describes the icons for the User Table page.

**Table 6-1 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 page.

- 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.

The following characters are not permitted in a username: ? . / ; [ ] { } " @ = !.

- 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.

The following characters are not allowed: ? ./;[]{}"!=

- 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, choose **Role Management**. The Role Management Table page is displayed.

Table 6-1 describes the icons for the Role Management page.

**Table 6-2 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 6-5.

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 that 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, choose **Domain Management**. The Domain Management Table page is displayed.
- To add domains, see the “Creating, Editing, and Deleting Domains” section on page 6-6.

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 that 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 VDS-IS 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, follow these steps:

---

**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 that you want to enable for this role. To choose all of 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 VDS-IS network entities or objects that make up the VDS-IS network. Whereas a role defines which services a user can perform in the VDS-IS 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, follow these steps:

- 
- 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 is displayed indicating that the entity type has not been assigned.
  - Step 7** From the left-panel menu, choose **Entity Management**. The Entity Management page is displayed.
  - Step 8** Click the **Assign** icon (blue cross mark) next to each entity name that 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.

### Creating a Domain Example

The following is an example of the tasks used to create a domain for a non-administrator user to be able to see a playlist view and have rights access to the SE, Delivery Service, and device group assigned to the playlist:

1. Choose **System > AAA > Domains**, and create a domain for entity type Delivery Services. Make sure that the Delivery Service the playlist uses is assigned to this domain.
2. Choose **System > AAA > Domains**, and create a domain for entity type Service Engine. Make sure that the SE the playlist uses is assigned to this domain.
3. Choose **System > AAA > Domains**, and create a domain for entity type Device Group. Make sure that the Device Group the playlist uses is assigned to this domain.
4. Choose **System > Users**. Select a user and assign the domains only configured to this user.

The non-administrator user should be able to see the playlist.

## Viewing Locked Users

If you login as an administrator, you can see a list of locked users along with the type of user and the time. The administrator can also unlock a user account.

To view or unlock a user account, follow these steps:

---

**Step 1** Choose **System > AAA > Locked users**. The Locked Users page is displayed.

**Step 2** Click **Unlock** hyperlink, to unlock a user account.

---

## Changing a Password

If you login as a user, 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.



**Note** If you login to the CDSM with built-in username(*admin*) and the initial password (*default*), you cannot change the password in the CDSM. However, you can change the password using CLI. The password expiry enhancement is not available for users logged in through built-in username and password.



**Caution**

It is not recommended to change 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, follow these steps:

---

**Step 1** Choose **System > Password**. The Password page is displayed.

**Step 2** In the **New Password** field, enter the changed password.

The following characters are not allowed: ?./;[]{}"=@=|

**Step 3** In the **Confirm New Password** field, re-enter the password for confirmation.

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

---

Starting from Release 4.0, the CDSM includes the following enhancements

- If you login as a user, the system home page will display the password expiration details.
- The CDSM prompts the user to change the password, if the password expires.

The following fields must be filled when the CDSM prompts you to change the password:

- Username—Name of the user.
- Password—User password.
- Confirm Password—Re-enter user password.

## Configuring System Settings

- [System Properties, page 6-8](#)
- [Configuring Device Offline Detection, page 6-10](#)
- [Configuring Distribution QoS, page 6-10](#)
- [Configuring Service Routing, page 6-12](#)
- [Authorization File Registration, page 6-15](#)
- [NAS File Registration, page 6-16](#)
- [HTTPS Settings, page 6-17](#)
- [Configuring the CDSM to Communicate with an External System, page 6-23](#)

## System Properties

To modify the system properties, follow these steps:

- 
- Step 1** Choose **System > Configuration > System Properties**. The System Properties page is displayed.
  - Step 2** Click the **Edit** icon next to the system property that 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 6-3](#) describes the system properties.

**Table 6-3 System Properties Fields**

Field	Description
cdsm.gui.rowCount	Row count for all pages containing table. The default is 10.
cdsm.password.expiry.days	The number of days for password expiry. The default is 0. The range is from 0 to 365.  <b>Note</b> The password will not expire if the value is set to 0.
cdsm.password.warning.days	The number of days for password expiry warning. The default is 30. The range is from 0 to 100.  <b>Note</b> The password warning message is not displayed if the value is set to 0.
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 (enable or disable).

**Table 6-3 System Properties Fields (continued)**

Field	Description
System.CmsUnsProgramSync.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.
System.device.recovery.key	Device identity recovery key. This property enables a device to be replaced by another node in the VDS network.
System.healthmonitor.collectRate	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 (enable or disable). This property allows settings that are configured using the local device CLI or the CDSM to be stored as part of the VDS-IS network configuration data.
System.monitoring.collectRate	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.dailyConsolidationHour	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 (enable or disable).
System.monitoring.monthlyConsolidationFrequency	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.recordLimitDays	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.updateEnabled	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.updateRateSec	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.  <b>Note</b> The rep_status_failed alarm gets triggered if the replication misses three times in a row. You can configure a lower value for the System.repstatus.updateRateSec to have the alarm trigger sooner.
System.repstatus.updateSyncEnabled	Sending summary replication status with requested detailed status (enable or disable).
System.security.minLength	Minimum number of characters required for a user password. The default is 6. The range is from 6 to 31.
System.security.minLength	Minimum number of characters required for a user name. The default is 4. The range is from 1 to 32.

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

## Configuring Device Offline Detection

Communication between all devices and the CDSM use User Datagram Protocol (UDP), which allows for fast detection of devices that have gone offline. UDP heartbeat packets are sent at a specified interval from each SE to the primary CDSM in a VDS-IS 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 non-responsive SEs as offline.



**Note** In VDS-IS 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 Device Offline Detection, follow these steps:

- Step 1** Choose **System > Configuration > Device Offline Detection**. The Configure Device Offline Detection page is displayed.



**Note** The Device Offline Detection feature is in effect only when the CDSM receives the first UDP heartbeat packet from an SE. UDP port of the heartbeat on the CDSM must be reachable for all devices; otherwise, the device shows as offline.

- Step 2** In the **Heartbeat Rate** field, specify how often, in seconds, the SEs should transmit a UDP heartbeat packet to the CDSM. The default is 10. The range is from 5 to 3600.

- Step 3** 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 3. The range is from 1 to 100.



**Note** Decreasing the heartbeat interval (**Heartbeat Rate \* Heartbeat Fail Count**) may take twice the original configured time to take effect. During this time, the online device status is not changed to “Offline” or “Online [Waiting for data feed].”

- Step 4** 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:

$$\text{Maximum Offline Detection Time} = \text{Heartbeat Rate} * \text{Heartbeat Fail Count}$$

- Step 5** 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 of 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, follow these steps:

- 
- 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 (DSCP) value from the **QoS value with low priority** drop-down list. Alternatively, enter a decimal value in the corresponding field.
- 
- Note** See the “[Setting DSCP Values for QoS Packets](#)” section on page 6-11 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 5-16 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 VDS-IS 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 6-4](#).)

**Note**

DSCP marking for Flash Media streaming is configured differently by Service Rule file.

**Table 6-4 DSCP Values**

<b>Keyword</b>	<b>Description and Value</b>
<b>af11</b>	Sets packets with AF11 DSCP (001010). <b>Note</b> The number in parentheses denotes the DSCP value for each per-hop behavior keyword.
<b>af12</b>	Sets packets with AF12 DSCP (001100).
<b>af13</b>	Sets packets with AF13 DSCP (001110).
<b>af21</b>	Sets packets with AF21 DSCP (010010).
<b>af22</b>	Sets packets with AF22 DSCP (010100).
<b>af23</b>	Sets packets with AF23 DSCP (010110).
<b>af31</b>	Sets packets with AF31 DSCP (011010).
<b>af32</b>	Sets packets with AF32 DSCP (011100).
<b>af33</b>	Sets packets with AF33 DSCP (011110).
<b>af41</b>	Sets packets with AF41 DSCP (100010).
<b>af42</b>	Sets packets with AF42 DSCP (100100).
<b>af43</b>	Sets packets with AF43 DSCP (100110).
<b>cs1</b>	Sets packets with CS1 (precedence 1) DSCP (001000).
<b>cs2</b>	Sets packets with CS2 (precedence 2) DSCP (010000).
<b>cs3</b>	Sets packets with CS3 (precedence 3) DSCP (011000).
<b>cs4</b>	Sets packets with CS4 (precedence 4) DSCP (100000).
<b>cs5</b>	Sets packets with CS5 (precedence 5) DSCP (101000).
<b>cs6</b>	Sets packets with CS6 (precedence 6) DSCP (110000).
<b>cs7</b>	Sets packets with CS7 (precedence 7) DSCP (111000).
<b>default</b>	Sets packets with the default DSCP (000000).
<b>ef</b>	Sets packets with EF DSCP (101110).

## Configuring Service Routing

The Service Routing menu options consist of the following:

- [Coverage Zone File Registration, page 6-12](#)
- [Configuring Global Routing, page 6-14](#)

### 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 “[Coverage Zone File](#)” section on page 1-38.

See [Appendix C, “Creating Coverage Zone Files,”](#) for information about creating a Coverage Zone file.

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 VDS-IS 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 of 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 of 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 VDS-IS 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, follow these steps:

- 
- 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 that 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, or FTP 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 6-5](#) describes the upload method fields. [Table 6-6](#) describes the import method fields.

**Table 6-5 Upload Method for Coverage Zone Files**

Property	Description
Coverage Zone File Upload	Local directory path to the Coverage Zone file. To locate the file, click <b>Browse</b> . Click <b>Validate</b> 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 6-6 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 <b>Validate</b> 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.

- 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, follow these steps:

- 
- 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.
- 

To apply a Coverage Zone file to an individual SR for local coverage zone configuration, see the “Configuring the Service Router” section on page 4-99.

## Authorization File Registration

The Authorization File Registration page is used to register a Service Rule file to the VDS-IS. A Service Rule file is associated with one or more delivery services. Each Delivery Service can have its own unique Service Rule file or multiple delivery services can have the same Service Rule file.

A Service Rule must be selected for a Delivery Service. For more information about Service Rule files, see [Appendix E, “Creating Service Rule Files.”](#) To select a Service Rule file for a Delivery Service, you first need to register the Service Rule file in the CDSM.

To register a Service Rule file, follow these steps:

- 
- Step 1** Choose **System > Configuration > Authorization File Registration**. The Authorization Plugin Files Table page is displayed.
- Step 2** Click the **Create New** icon in the task bar. The Registering Service Rule File page is displayed. To edit a Service Rule file registration, click the **Edit** icon next to the registration that you want to edit.
- Step 3** Choose a file import method from the **File Import Method** drop-down list:
- **Import**—The import method allows you to import an XML file from an external HTTP, HTTPS, or FTP server.
  - **Upload**—The upload method allows you to upload an XML file from any location that is accessible from your PC by using the browse feature.
- 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 6-5](#) describes the upload method fields. [Table 6-6](#) describes the import method fields.

**Table 6-7      Upload Method for XML Files**

Property	Description
File Type	From the <b>File Type</b> drop-down list, choose <b>Rule File</b> .
Source File Upload	Local directory path to the file. To locate the file, click <b>Browse</b> . Click <b>Validate</b> to validate the XML file.
Destination Filename	Name of the file. This field is filled in automatically with the filename from the local directory path.

**Table 6-8      Import Method for XML Files**

Property	Description
File Type	From the <b>File Type</b> drop-down list, choose <b>Rule File</b> .
File URL	The URL where the file is located, including path and filename. Click <b>Validate</b> to validate the XML file.
Destination File Name	Name of the file.
Update Interval (minutes)	Frequency with which the CDSM looks for changes to the file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the file.
Password	User password for fetching the file.

- Step 5** To save the settings, click **Submit**.
- 

## NAS File Registration

A NAS file is associated with the SEs in the root location of a Delivery Service. One SE in the root location of a Delivery Service acts as the Content Acquirer. The NAS file is associated with the Delivery Service by assigning the file to the content origin. Each content origin can have its own unique NAS file or multiple content origins can have the same NAS file.



- Note** NAS is only supported in lab integrations as proof of concept.
- 

For information about assigning a NAS file to a content origin, see the “Content Origins” section on page 5-1. For information about creating a NAS file, see Appendix G, “Creating NAS Files.” To assign a NAS file to a content origin, you first need to register the file in the CDSM.

To register a NAS file, follow these steps:

- 
- Step 1** Choose **System > Configuration > NAS File Registration**. The NAS File Table page is displayed.
- Step 2** Click the **Create New** icon in the task bar. The File Registration page is displayed.
- To edit a NAS file registration, click the **Edit** icon next to the registration that 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 NAS file from any location that is accessible from your PC by using the browse feature.
  - **Import**—The import method allows you to import a NAS file from an external HTTP, HTTPS, or FTP 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 6-5 describes the upload method fields. Table 6-6 describes the import method fields.

**Table 6-9      Upload Method for XML Files**

Property	Description
Source File Upload	Local directory path to the file. To locate the file, click <b>Browse</b> . Click <b>Validate</b> to validate the XML file.
Destination Filename	Name of the file. This field is filled in automatically with the filename from the local directory path.

**Table 6-10 Import Method for XML Files**

Property	Description
File URL	The URL where the file is located, including path and filename. Click <b>Validate</b> to validate the XML file.
Destination File Name	Name of the file.
Update Interval (minutes)	Frequency with which the CDSM looks for changes to the file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the file.
Password	User password for fetching the file.

- Step 5** To save the settings, click **Submit**.
- 

## HTTPS Settings

Certificate Authority's (CA's) root certificates are expected to be available to all clients initiating HTTPS communication; most browsers are installed with well-known CA root certificates. Trusted CA certificates are expected to be provided for the purpose of Origin server and Client certification validation.



**Note** A single subject alternative name (SAN) certificate is installed for all delivery services in the VDS-IS.

For more information about HTTPS Settings and how to configure it, see the “[“HTTPS Settings” section on page 2-25](#)” section

Uploading certificate and key files consists of the following pages:

- **Root CA File Registration**—Upload or import the certificates for the Origin servers participating in HTTPS
- **CRL File Registration**—Upload the CRL certificates for the Service Engine participating in HTTPS
- **CRL File Scheduling**—Schedule CRL file notification to the Web Engine on each SE that is participating in an HTTPS Delivery Service
- **HTTPS Certification Files Registration**—Upload client certificate and key file for all SEs
- **HTTPS Certification File Scheduling**—Schedule client certificate and key file notification to the Web Engine on each SE that is participating in an HTTPS Delivery Service

The procedures involved in uploading certificate and key files consist of the following:

- [Configuring HTTPS General Settings](#)
- [Uploading or Importing a Root CA File](#)[Uploading a CRL File](#)[Scheduling a CRL File](#)
- [Uploading Certificate and Key Files](#)
- [Scheduling Web Engine Notification of Certificate and Key Files](#)

## Configuring HTTPS General Settings

Starting with Release 3.3, The CDSM GUI offers the ability to enable HTTPS or HTTP for streaming to clients as well as ingesting from the Origin server for each Delivery Service.

To configure the HTTPS settings, follow these steps:

- 
- Step 1** Choose **System > Configuration > HTTPS Settings > General Settings**. The HTTPS General Settings is page displayed.
- Step 2** Enter the settings as appropriate. See [Table 6-11](#) for a description of the fields.

**Table 6-11 General Setting Fields**

Field	Description
Delivery Streaming Mutual Authentication	Check the <b>Delivery Streaming Mutual Authentication</b> check box to enable delivery streaming mutual authentication for the individual Delivery Service. The default is unchecked.
Delivery Streaming Supported Cipher List	<p>Input the Cipher list. The default is empty.</p> <p>When the Web Engine is acting as an HTTPS server, the <b>Delivery Streaming Supported Cipher List</b> is used to negotiate and accept HTTPS connections from the client player.</p> <p><b>Note</b> When it is empty, the backend will use the default string.</p>

- 
- Step 3** Click **Validate**, to verify if the cipher list is valid.
- Step 4** Click **Submit** to save the settings.
- 

## Uploading or Importing a Root CA File

The root certificates are used by SEs to validate the Origin server certificates, one or more root certificates can be uploaded to the CDSM.

After a new root certificate is uploaded to the CDSM, it is distributed to all SEs immediately. The SE does not notify the Web Engine of the existence or update of a root certificate file; instead, the Web Engine fetches them when necessary.

To upload or import a root CA file, follow these steps:

- 
- Step 1** Choose **System > Configuration > HTTPS Settings > Root CA File Registration**. The Root CA File Registration table is displayed.
- Step 2** Click the **Create New** icon in the task bar. The File Registration page is displayed.
- To edit a root CA file, click the **Edit** icon next to the file that you want to edit.
- Step 3** Choose a file import method from the **File Import Method** drop-down list:
- **Upload**—Uploads a file from any location that is accessible from your PC using the browse feature.

- **Import**—Imports a file from an external HTTP, HTTPS, or FTP 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 6-12](#) describes the upload method fields. [Table 6-13](#) describes the import method fields.

**Table 6-12 Upload Method for Root CA Files**

Property	Description
Source File Upload	Local directory path to the file. To locate the file, click <b>Browse</b> .
Destination Filename	Name of the file. This field is filled in automatically with the filename from the local directory path.

**Table 6-13 Import Method for Root CA Files**

Property	Description
File URL	The URL where the file is located, including path and filename.
Destination File Name	Name of the file.
Update Interval (minutes)	Frequency with which the CDSM looks for changes to the file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the file.
Password	User password for fetching the file.

**Step 5** To save the settings, click **Submit**.

---

## Uploading a CRL File

A Certification Revocation List (CRL) is a list of certificates that is revoked before their scheduled expiration date. It is maintained by a CA, and it provides information about revoked certificates that were issued by that CA. After uploading the CRL file from the CA, it should be imported into the SE.

To upload and schedule the CRL files, follow these steps:

- Step 1** Choose **System > Configuration > HTTPS Settings > CRL File Registration**. The CRL File Registration File page is displayed.
- Step 2** Click the **Create New** icon in the task bar. The File Registration page is displayed.  
To edit a root CRL file, click the **Edit** icon next to the file that you want to edit.
- Step 3** Choose a file import method from the **File Import Method** drop-down list:
  - **Upload**—Uploads a file from any location that is accessible from your PC using the browse feature.
  - **Import**—Imports a file from an external HTTP, HTTPS, or FTP 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 6-14](#) describes the upload method fields. [Table 6-15](#) describes the import method fields.

**Table 6-14 Upload Method for CRL Files**

Property	Description
Source File Upload	Local directory path to the file. To locate the file, click <b>Choose File</b> .
Destination Filename	Name of the file. This field is filled in automatically with the filename from the local directory path.

**Table 6-15 Import Method for CRL Files**

Property	Description
File URL	The URL where the file is located, including path and filename.
Destination File Name	Name of the file.
Update Interval (minutes)	Frequency with which the CDSM looks for changes to the file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the file.
Password	User password for fetching the file.

- Step 5** To save the settings, click **Submit**.

## Scheduling a CRL File

After the CRL files have been uploaded to the CDSM and distributed to all of the SEs in the system, the Web Engine on each SE participating in an HTTPS Delivery Service needs to be notified of the newly uploaded CRL files.

To schedule Web Engine notification of certificate and key files, follow these steps:

- 
- Step 1** Choose **System > Configuration > HTTPS Settings > CRL File Schedule**. The Scheduling Tasks table is displayed.
- Step 2** Click the **Create New** icon in the task bar. The Certificate Schedule Task page is displayed. The table lists the scheduled tasks, the SEs assigned to that task, and the status of the task (expired or active). To edit a schedule, click the **Edit** icon next to the schedule that you want to edit. Expired tasks cannot be edited.
- Step 3** To schedule the task to run immediately, check the **Immediately Run** check box.

To schedule the task to run at a specific date and time, follow these steps:

- a. Click the **Calendar** icon next to the **Schedule Date and Time** field to enter the date and time. The Calendar dialog box is displayed.
- b. From the **Month** drop-down list, choose the month.
- c. To change the year, use the right arrow and left arrow on either side of the current year.
- d. To select the day of the month, click the day in the calendar displayed. The current date is highlighted in yellow.
- e. In the **Time** field, using the 24-hour clock, enter the time of day.

To reset the date and time to today, click **Set Today**.

- f. Click **Apply**. The date and time you selected is entered in the **Schedule Date and Time** field.

**Step 4** Click the **Assign** icon (blue cross mark) next to the SE that you want to assign to this task. Alternatively, in the task bar, click **Assign All Service Engines**. The SE assignment states are described in [Figure 6-2](#).

**Figure 6-1 Content Origin Assignment State**

New Assign	Assigned and waiting for Submit	Assignment Submitted	Unassign Submitted Assignment

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 5** To schedule the task, click **Submit**. The task is displayed in the Scheduling Tasks table.

To delete all expired tasks from the Scheduling Tasks table, click the **Delete All** icon. To delete a specific task, click the **Edit** icon next to the task that you want to delete, and when the task is displayed, click the **Delete** icon.

## Uploading Certificate and Key Files

The certificate and key files are uploaded to the CDSM, then the CDSM immediately distributes them to all of the SEs in the system. The certificate and key file distribution is independent of notifying the Web Engine of the newly uploaded certificate and key files, which occurs based on the defined schedule or immediately if the **Immediately Run** check box is checked.

One pair of certificate and key files are used by all SEs in the system to send to HTTPS clients for authentication. Uploading new certificate and key files overwrites the existing ones. The certificate and key files work as a pair, so updating one of them requires the other one be updated as well.

To upload the client certificate and key files, follow these steps:

- Step 1** Choose **System > Configuration > HTTPS Settings > HTTPS Certification Files Registration**. The HTTPS Certification File page is displayed.
- Step 2** To upload a certificate file, click the **Browse** button for the Certification File and navigate to the file.
- Step 3** To upload a key file, click the **Browse** button for the Key File and navigate to the file.
- Step 4** To save the settings, click **Submit**.

To delete a certificate or key file, click the **Delete** icon next to the file type. Deleting a certificate file or key file deletes the file from the CDSM and all SEs in the system, and impacts the HTTPS feature. The files should only be deleted if the HTTPS feature is no longer used. File deletion can only occur when there are no active HTTPS certificate file tasks scheduled.

## Scheduling Web Engine Notification of Certificate and Key Files

After the certificate and key files have been uploaded to the CDSM and distributed to all of the SEs in the system, the Web Engine on each SE participating in an HTTPS Delivery Service needs to be notified of the newly uploaded certificate and key files.

To schedule Web Engine notification of certificate and key files, follow these steps:

- 
- Step 1** Choose **System > Configuration > HTTPS Settings > HTTPS Certification Files Schedule**. The Scheduling Tasks table is displayed.
- Step 2** Click the **Create New** icon in the task bar. The Certificate Schedule Task page is displayed. The table lists the scheduled tasks, the SEs assigned to that task, and the status of the task (expired or active). To edit a schedule, click the **Edit** icon next to the schedule that you want to edit. Expired tasks cannot be edited.
- Step 3** To schedule the task to run immediately, check the **Immediately Run** check box. To schedule the task to run at a specific date and time, follow these steps:
- Click the **Calendar** icon next to the **Schedule Date and Time** field to enter the date and time. The Calendar dialog box is displayed.
  - From the **Month** drop-down list, choose the month.
  - To change the year, use the right arrow and left arrow on either side of the current year.
  - To select the day of the month, click the day in the calendar displayed. The current date is highlighted in yellow.
  - In the **Time** field, using the 24-hour clock, enter the time of day.
- To reset the date and time to today, click **Set Today**.
- Click **Apply**. The date and time you selected is entered in the **Schedule Date and Time** field.
- Step 4** Click the **Assign** icon (blue cross mark) next to the SE that you want to assign to this task. Alternatively, in the task bar, click **Assign All Service Engines**. The SE assignment states are described in [Figure 6-2](#).

**Figure 6-2 Content Origin Assignment State**

New Assign	Assigned and waiting for Submit	Assignment Submitted	Unassign Submitted Assignment

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 5** To schedule the task, click **Submit**. The task is displayed in the Scheduling Tasks table.

To delete all expired tasks from the Scheduling Tasks table, click the **Delete All** icon. To delete a specific task, click the **Edit** icon next to the task that you want to delete, and when the task is displayed, click the **Delete** icon.

## Configuring the CDSM to Communicate with an External System

CDSM can be configured to communicate with external systems. Currently, Prime Central is supported as one type of external system.

Cisco PRIME for service providers is an experience delivery management architecture that enables the integrated design, fulfillment and assurance of customer experiences such as video, mobility, and managed cloud services delivered on converged IP networks.

As part of Cisco PRIME, the CDSM forwards alarms as SNMP traps to Prime Central. The CDSM supports the following functionality to provide communication to Prime Central:

- CDSM configuration settings to allow communication with Prime Central
- Registration of the CDSM on Prime Central
- Sending SNMP traps to Prime Central

### Registering and De-Registering with Prime Central

The CDSM registers with Prime Central by checking **Register** check box in the External System page.

The registration process takes about 10 to 20 seconds. After registration is complete, the CDSM updates the status (Registered or Registration Failed) of Prime Central.

**Note**

CDSM should be de-registered from the Prime Central before deleting the configuration settings of Prime Central. Excluding **Fault Manager Server IP** and **Fault Manager Server Port** fields, the configuration settings of the Prime Central listed in [Table 6-16](#) cannot be modified when the status is Registered.

To configure the settings for an external system (Prime Central), follow these steps:

- Step 1** From the CDSM GUI, choose **System > Configuration > External Systems**. The External Systems table is displayed.
- Step 2** Click the **Create New** icon in the task bar. The External System page is displayed.  
To edit an external system, click the **Edit** icon next to the external system name.
- Step 3** Enter the settings as appropriate. See [Table 6-16](#) for a description of the fields.

**Table 6-16      External System Parameters**

Field	Description
Name	Name of the External System
Type	Prime Central is the only option.

**Table 6-16 External System Parameters (continued)**

Field	Description
Status	Registration status, It can have the following values: Registered Unregistered Registering Registration Failed Deregistering
Register	Check the <b>Register</b> check box to register the CDSM with Prime Central.
IP address	IP address of the Prime Central.
Database SID	Database schema ID of the Prime Central.
Database Port	Database Port Number of the Prime Central.
Database User	Database User Name of the Prime Central.
Database Password	Database Password of the Prime Central.
Fault Manager Server IP	IP address of the Prime Central Fault Manager, used by CDSM to send SNMP traps to the Prime Central.
Fault Manager Server Port	Port number of the Prime Central Fault Manager, used by CDSM to send SNMP traps to the Prime Central.
Comments	Description of the External System.

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

---

## Viewing or Downloading XML Schema Files

The XML Schema Files page provides links to the XML schema files for viewing or downloading. All XML files can be validated through the CDSM by clicking **Validate** on the associated CDSM page. However, if you want to use an external XML validation program, you can save the XML schema file to use for that purpose. The following XML schema files are available:

- CDSAutorization.xsd—Geo/IP file used to specify the geographic regions and IP networks that are allowed or denied access to a Delivery Service.
- CDSRules.xsd—Service Rule file used by a Delivery Service to specify the Service Rules for all SEs in a Delivery Service.
- CdsCoverageZone.xsd—Coverage Zone file is used to customize the networks and geographic regions each SE services.
- CdsOrigin.xsd—NAS file used for defining a NAS device.
- CdnManifest.xsd—Manifest file is used to specify the content to be prefetched and to control the delivery of the prefetched content for a Delivery Service.
- ContentDeletionTask.xsd—Content Deletion Task file is used to specify the content to be deleted for delivery services.

To open or save an XML schema file, follow these steps:

- 
- Step 1** Choose **System > CDS-IS Files > XML Schema Files**. The CDS-IS XML Schema page is displayed with a link to each XSD (schema) file.
- Step 2** Click the link for the file. Depending on the browser program used, one of the following or something similar happens:
- The file is displayed in a new page and the File Download dialog box is also displayed.
  - The opening dialog box is displayed.
  - The file is displayed in a text editor program.
-

**■ Viewing or Downloading XML Schema Files**



# Configuring Licenses

This chapter provides information on configuring licenses for the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS).

- [Viewing CDN License Summary, page 7-2](#)
- [Configuring License Files, page 7-3](#)
- [Purchase Information, page 7-3](#)
- [License Logs, page 7-4](#)

Starting with Release 4.0, VDS-IS introduces three types of licenses:

- Application License—The application license defines the role of a device.
- Advanced Feature License—The advanced feature license defines the advanced features.
- Capacity License—The capacity license defines the CDN capacity like bandwidth and TPS.

The VDS-IS also introduces 2 types of license modes for the licenses:

- Perpetual Mode
- Annual Mode

The streaming capacity license supports both the perpetual mode and annual mode. The other licenses supports only the perpetual mode.

## Application License Enforcement

The CDSM automatically assigns the devices a few application licenses. If the number of purchased licenses are not sufficient, the CDSM raises an alarm for the devices for a grace period of 60 days. After 60 days, if you fail to purchase enough licenses, the CDSM will do the following enforcement for those devices:

- The CDSM will not allow the use of a streamer while creating a new Delivery Service.
- If a Streamer exceeds the 60 days grace period, the device group which includes this device cannot be assigned to a Delivery Service.
- For R-VDSISBU20, by which the CDSM can only manage up to 20 streamers, the CDSM should reject any SE registration, if the managed SE count exceeds 20.

## Capacity License Enforcement

The CDSM provides a 60 day grace period to purchase enough capacity licenses. After 60 days, if you fail to purchase enough licenses, the CDSM will do the following enforcement for those devices:

- The CDSM will block the operation of adding new streamers to the Delivery Service with a suitable message that the streaming capacity license needs to be purchased, every time you try to add a streamer.
- The CDSM will block the creation of new delivery service with a suitable message that the streaming capacity license needs to be purchased, every time you try to create a Delivery Service.
- The CDSM will block the operation of adding new a device group to the Delivery Service with a suitable message that the streaming capacity license needs to be purchased, every time you try to assign a device group.
- The CDSM will block the operation of adding new a streamer to a device group when this device group already assigned into the Delivery Service with a suitable message that the streaming capacity license needs to be purchased

**Note**

Currently, the following licenses have no enforcements:

- Advance Feature Licenses
- SR TPS Licenses
- Proximity TPS Licenses

However, an alarm is raised if you fail to purchase enough licenses.

## Viewing CDN License Summary

The CDN License Summary page displays all the license files used by the system.

To view the CDN License Summary, follow these steps:

**Step 1** Choose **Licenses > CDN License Summary**. The CDN License Summary page is displayed.

**Table 7-1** describes the CDN License Summary 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 7-1      CDN License Summary Columns**

Column Heading	Description
License Category	License category name.
Type	License category type: Application, Feature, Capacity.
License Quantity	License quantity registered in the CDN system.
Needed Quantity	Needed license. For license categories whose type is Capacity, the Needed Quantity column displays NA.
Status	License category status: Normal, Violated.
Last Modification Time	Timestamp of the latest update for the license category as recorded on the uploaded license.

- Step 2** Click the **View** icon (the eyeglasses icon) next to the license category.
- License Detail—The **License Detail** page, displays the Purchased product ID, along with the purchased quantity, valid quantity, and the license quantity.
  - License Usage—The **License Usage** page, displays the device name, along with the device type, need license, license assigned, and status.
- 

## Configuring License Files

If you login as a user, you can see the purchase information if you meet the following requirements:

- You must have already got license files from vendor
- Unzip the license files
- Save the license files in any location that is accessible from your PC using the browse feature.

To register a License file, follow these steps:

- 
- Step 1** Choose **Licenses > License Files**. The License File page is displayed.
- Step 2** Click the **Create New** icon in the task bar. The Registering License File page is displayed. To edit a License file registration, click the **Edit** icon next to the registration you want to edit.
- Step 3** To upload a license file, click the **Choose File** or **Browse** button for the License File and navigate to the file.
- Step 4** In the **Destination Filename** field, enter the file name.
- Step 5** To save the settings, click **Submit**.
- 

## Purchase Information

The Purchase Information page displays the Purchased Product IDs.

To view the Purchase Information, follow these steps:

- 
- Step 1** Choose **Licenses > Purchase Information**. The Purchase Information page is displayed.
- Table 7-2** describes the Purchase Information 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 7-2 Purchase Information Columns**

Column Heading	Description
Product ID	Purchased Product ID.
Type	License category type: Application, Feature, Capacity.

**Table 7-2 Purchase Information Columns**

Column Heading	Description
Quantity	Number of purchased Product IDs.
Expired Date	Expiration timestamp for annual licenses.
Description	Description for license.
Status	Purchased Product ID status: Valid, Invalid, Expired.
Error Message	Error information.

- Step 2** Click the **View** icon (the eyeglasses icon) next to the Product ID.

- Purchase Information—The **Purchase Information** page displays the PAK, along with the quantity, expired date, status, and error message details.

**Table 7-3** describes the icons for the purchased product IDs table. To view the purchase information for the license, click the View (eyeglasses) icon next to the product ID.

**Table 7-3 Purchase Information Icons**

Icon	Function
	Export a table to a comma-separated value (CSV) file.
	Create a filtered table. Filter the license features by the Product ID, and Type.
	View all Purchased Product IDs. Click this icon to view all the Purchased Product IDs after you have created a filtered table.
	Refresh the table
	Print the current window.

## License Logs

The CDSM logs license activity in the system. The only activities that are logged are those that change the VDS-IS network. This feature provides accountability for user actions (for example, which user did what and when). Logged activities include the following:

- After 60 days of expiration, when a PAK annual capacity license is removed from the system.

To view license logs, follow these steps:

- Step 1** Choose **Licenses > License Logs**. The License 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.
-





# Monitoring the Videoscape Distribution Suite, Internet Streamer

---

The Content Delivery System Manager (CDSM) provides tools that can be used for system monitoring and system diagnostics.

- [System Monitoring, page 8-1](#)
- [Device Monitoring, page 8-13](#)
- [Reports, page 8-26](#)
- [Delivery Service Monitoring, page 8-30](#)
- [Viewing Statistics, page 8-44](#)
- [Log Files, page 8-54](#)
- [Transaction Logs, page 8-54](#)

## System Monitoring

System monitoring consists of the following:

- [System Status, page 8-1](#)
- [System Home Page, page 8-7](#)
- [System Audit Logs, page 8-9](#)
- [System Port Numbers, page 8-10](#)

## System Status

The CDSM displays the system status in the System Status bar that is located above the navigation tabs in every page. The System Status bar presents the overall device and content health of the system. You can use this feature to monitor devices and content replication in your Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS) network. The System Status bar helps you immediately identify any problems on the network, allowing you to act and respond to problems quickly.

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)

**System Monitoring**

- Yellow—Minor alarms
- Orange—Major alarms
- Red—Critical alarms

When you hover your mouse cursor over an alarm light in the System Status bar, a pop-up message provides further details about the device or Delivery Service. See [Figure 8-1](#).

The icon next to the System Status either displays a yellow triangle with an exclamation mark or a green circle with a check mark. The yellow triangle indicates the alarms and alerts count includes only the unacknowledged alarms and alerts. The green circle with a check mark indicates all alarms and alerts are counted, whether they are acknowledged or unacknowledged.

**Figure 8-1      System Status Bar**



When you click the alarm light or the link next to the alarm light, a new page opens (Troubleshooting Devices or Troubleshooting Service), listing the individual devices or delivery services that need attention.

**Figure 8-2      Troubleshooting Devices Page**

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	
⚠				🟡🟡🟡	Major: SE DD4-FIBER-1 keeps	Troubleshooting DD4-CDE220-2 : Edit/Monitor Device	0:35:16 GMT 2010
⚠	U1-2S3-1	7.5.1.13	Online	🟡🟡🟡	Major: Device clock is not syn	Telnet to Device	
⚠				🟡🟡🟡	CDSM. Enabling NTP on all the	Run Show Commands	8:53:40 GMT 2010
⚠	DD4-FIBER-1	8.1.0.8	Online	🟡🟡🟡	Major: Core file(s) detected		Fri May 07 19:51:10 GMT 2010
⚠				🟡🟡🟡	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		Set May 15 00:32:59 GMT 2010
⚠				🟡🟡🟡	psu failed.		
⚠				🟡🟡🟡	Minor: "Device: /dev/sdd, 1 Currently unreadable		Set May 15 00:34:49 GMT 2010
⚠	U1-2S3-1	7.5.1.13	Online	🟡🟡🟡	(pending) sectors"		
⚠				🟡🟡🟡	Minor: A power supply power cable is unplugged or the		Tue Mar 16 21:03:40 GMT 2010
⚠	DD4-CDE205-1	8.1.0.5	Online	🟡🟡🟡	psu failed.		Thu May 13 19:13:55 GMT 2010
⚠	DD4-FIBER-1	8.1.0.8	Online	🟡🟡🟡	Minor: Some content or crawl jobs of delivery		
⚠				🟡🟡🟡	service:HTTP are failed to be acquired or replicated.		
⚠				🟡🟡🟡	Minor: A power supply power cable is unplugged or the		
⚠				🟡🟡🟡	psu failed.		Fri May 07 00:59:16 GMT 2010

#### Troubleshooting Window Pop-Up Menus

When you hover your mouse cursor over an item under the Alarm Information column in the Troubleshooting page, the Troubleshooting Tools menu is displayed. The Troubleshooting Tools menu provides links to all of the diagnostic tools, troubleshooting tools, and monitoring applications for troubleshooting and resolving the problem. [Figure 8-2](#) shows the Troubleshooting Tools menu for device alarms.

[Table 8-1](#) describes the icons for the Troubleshooting page.

**Table 8-1 Troubleshooting Page Icons**

Icon	Function
	Creates a filtered table. Filter the alarms by severity or device type.
	Views all alarms. Click this icon to view all alarms after you have created a filtered table.
	Refreshes the table.
	Prints the current window.
	Views acknowledged alarms.

You can sort the Troubleshooting table by clicking any column heading displayed in blue. The first time the column heading is clicked, the table is sorted by that column in the ascending order. If the column heading is clicked again, the table is sorted by that column in the descending order.



If there is more than one alarm for a device, and the Troubleshooting page is sorted by device, then the device is only listed once for multiple alarms associated with it. The same is true for service alarms.

#### Troubleshooting Page Acknowledge and Unacknowledge Alarms Function

To acknowledge and unacknowledge an alarm, follow these steps:

- Step 1** To remove an alarm from the Troubleshooting page, check the check box for the alarm. The alarm is moved to the Acknowledged Alarm page.
- Step 2** To view the acknowledged alarms, click the **View acknowledged alarms** icon. The Acknowledged Alarm page is displayed ([Figure 8-3](#)).

**Figure 8-3 Acknowledged Alarms Window**

Acknowledging Devices							Rows: 10	
	Device Name	IP Address	Status	Severity	Alarm Information	Time	Ack By	Ack When
	V8-CDE220-8	4.5.0.18	Online		Minor: A power supply power cable is unplugged or the psu failed.	Mon Oct 04 13:46:30 GMT 2010	admin	Tuesday, October 5, 2010 1:10:12 AM GMT
	V8-CDE220-1	4.5.0.2	Online		Minor: A power supply power cable is unplugged or the psu failed.	Thu Sep 30 08:10:43 GMT 2010	admin	Tuesday, October 5, 2010 1:10:07 AM GMT
	DD4-FIBER-1	8.1.0.8	Online		Minor: A power supply power cable is unplugged or the psu failed.	Thu Sep 30 16:52:19 GMT 2010	admin	Tuesday, October 5, 2010 1:09:58 AM GMT
	DD4-FIBER-1	8.1.0.8	Online		Minor: "Device: /dev/sdg, 1592 Currently unreadable (pending) sectors"	Thu Sep 30 16:53:31 GMT 2010	admin	Tuesday, October 5, 2010 1:09:52 AM GMT

<< Page 1 >>      Showing 1-4 of 4 Acknowledged Alarms

207306

**Step 3** To unacknowledge an alarm, check the check box for the alarm. The alarm is returned to the Troubleshooting page.

**Step 4** To view the Troubleshooting page again, click the **Back** (blue left arrow) icon.

## Device Alarms

Device alarms are associated with device objects and pertain to 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 keepalive timed out alarm) if the SE has a Layer 3 failure. Device alarms can also reflect reporting problems between the device and the CDSM. (See [Table 8-2](#).)

Alarm thresholds are configured for each device. For more information, see the “[Setting Service Monitor Thresholds](#)” section on page [4-83](#).

**Table 8-2 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.
Device has lower software version	Minor	Online	The device is not inter-operable with the CDSM because it has an earlier software version.

To troubleshoot a device from the System Status bar, follow these steps:

**Step 1** In the System Status bar, click the **Devices** alarm light or click the **Device** link. The Troubleshooting Devices page is displayed.

- Step 2** In the Alarm Information column, hover your mouse cursor over the alarm message until the Troubleshooting Tools menu is displayed. See [Figure 8-2](#).
- Step 3** Click the troubleshooting tool that you want to use. The link takes you to the corresponding page in the CDSM. [Table 8-3](#) describes the tools available for all device alarms.

**Table 8-3** *Troubleshooting Tools for Device Alarms*

Item	Navigation	Description
Edit/Monitor Device	Devices home page	Displays the 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 &gt; Monitoring &gt; Show/Clear Commands &gt; Show Commands</b>	Displays the device <b>show</b> command tool.
Core Dump File	<b>Devices &gt; Device &gt; Monitoring &gt; Core Dump Files</b>	Displays a list of core dump files on the device.
Update Software	<b>Devices &gt; Devices &gt; Device Home &gt; Update Software</b>	Displays a list of software files that have been uploaded to the VDS-IS.

## Service Alarms

Service alarms pertain to 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, follow these steps:

- Step 1** In the System Status bar, click the **Services** alarm light or click the **Service** link. The Troubleshooting Services page is displayed. [Table 8-4](#) lists the service alarms.

**Table 8-4** *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, hover your mouse cursor 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 8-5](#) describes the tools available for all service alarms.

**Table 8-5** *Troubleshooting Tools for Content Alarms*

Item	Navigation	Description
View Replication Status	<b>Services &gt; Delivery Services &gt; Replication Status</b>	Displays the 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

## License Alarms

License alarms are associated with the purchased licenses. License alarms are raised or cleared by the CDSM for the following reasons:

- Device registration and de-registration.
- Assigning or Un-assigning an SE from a Delivery Service.
- Configuration changes, if there are any.
- If the capacity usage including TPS and bandwidth exceeds the purchased license.



**Note** The ACK alarm functions are available for annual licenses and expired alarms.

To troubleshoot purchased license issues from the License bar, follow these steps:

- Step 1** In the License bar, click the **Licenses** alarm light or click the **License** link. The Troubleshooting Services page is displayed.
- Step 2** The Severity column lists the status of the license:
- Minor Alarm [1 to 20 days violation]—Minor alarms are raised for licenses with 1 to 20 days violation
  - Minor Alarm —Minor alarms are raised for annual licenses when it will expire within 90 days.
  - Major Alarm [21 to 40 days violation]—Major alarms are raised for licenses with 21 to 40 days violation.
  - Critical Alarm [41 to 60 days violation]—Critical alarms are raised for licenses with 41 to 60 days violation.
  - Critical Alarm—Critical alarms are raised for annual licenses when it expired within 60-days. After 60-days grace period, this alarm is cleared and the related PAK annual capacity license is removed from system with its capacity.
- Step 3** In the Alarm Information column, hover your mouse cursor over the alarm message until the Troubleshooting Tools menu is displayed.
- Step 4** From the Troubleshooting tools menu, follow one of these steps:

- Click the **View CDN License Summary**. The link takes you to the corresponding page in the CDSM.  
For more information about viewing CDN licenses, see the “[Viewing CDN License Summary](#)” section on page 7-2.
  - For annual license expiration alarm, click **View Purchase Information**. The link takes you to the corresponding page in the CDSM.  
For more information about viewing purchase information, see the “[Purchase Information](#)” section on page 7-3.
- 

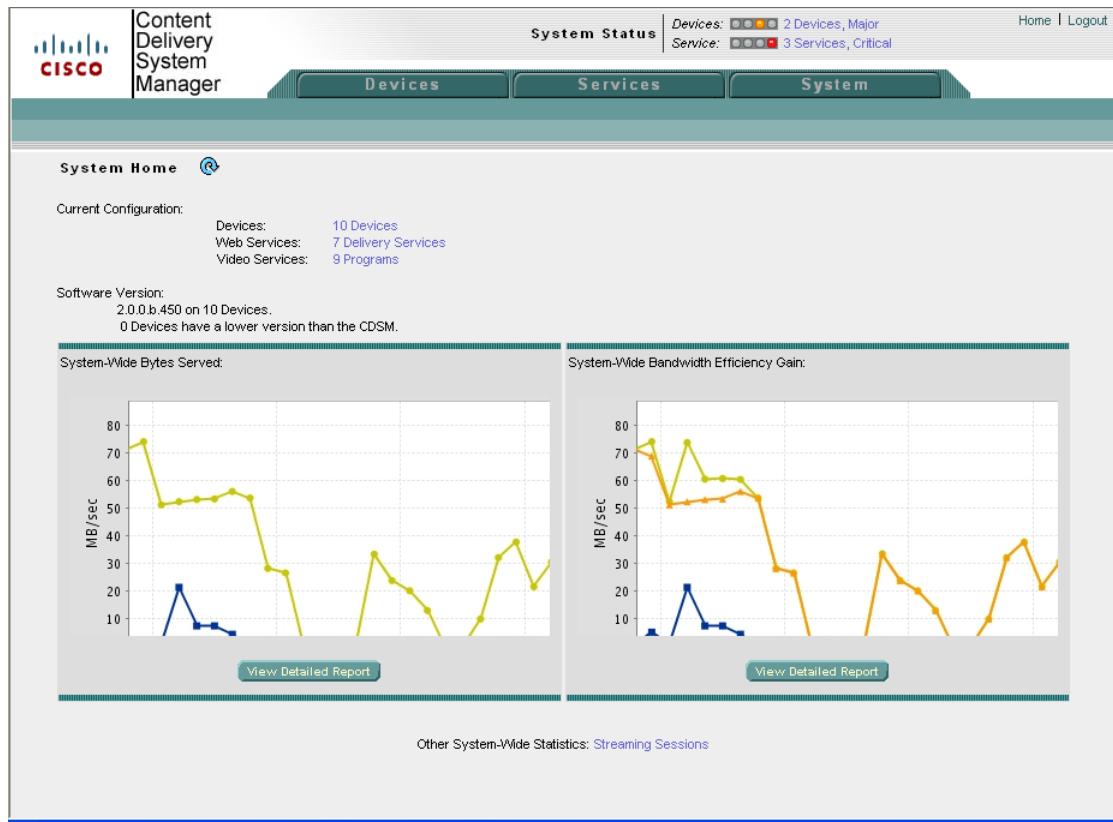
## System Home Page

The System Home page ([Figure 8-4](#)) provides overall system performance graphs, and overall system information on configuration and software versions running on the VDS-IS devices. Clicking the links for devices, delivery services, and programs take you to the corresponding table pages.



**Note** The number of devices that have a lower version of software than the CDSM only compares the major and minor release numbers (X.Y) of the software release number. The software release number consists of X.Y.Z-b#, where X is the major release number, Y is the minor release number, Z is the maintenance release number, and b# is the build number. Devices with a lower X.Y version than the CDSM do not interoperate with the CDSM, and the CDSM does not send configuration updates to those devices. A minor alarm is generated for the devices with a lower version of software.

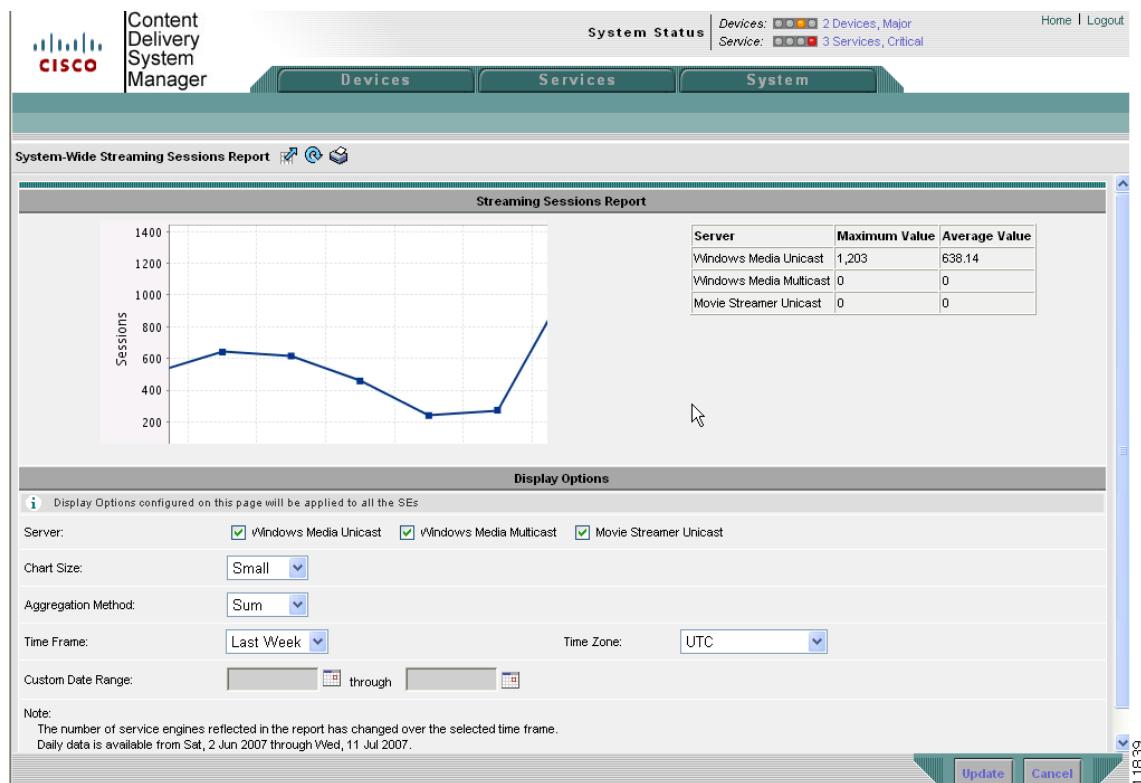
---

**Figure 8-4 System Home Page**

211836

The information displayed in the graphs is based on a snapshot of your VDS-IS network and represents the state of your SEs at the end of every two polling periods. To refresh the graphs, you can click the **Refresh** icon next to “System Home.” You can 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).

To change the report settings for the System-Wide Bandwidth Served or System-Wide Bandwidth Efficiency Gain graphs, click **View Detailed Report**. Clicking the **Streaming Sessions** link at the bottom of the home page opens the System-Wide Streaming Sessions Report page (Figure 8-5). For more information about these reports, see the “Reports” section on page 8-26.

**Figure 8-5 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 VDS-IS network. This feature provides accountability for users actions (for example, which user did what and when). Logged activities include the following:

- Creation of VDS-IS network entities
- Modification and deletion of VDS-IS network entities
- System configurations

To view audit trail logs, follow these steps:

- 
- 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 about all of the protocols and ports used by the VDS\_S can be viewed in the CDS-IS Well Known Ports page.

To view ports used by the VDS-IS, choose **System > CDS-IS Well Known Ports**. The CDS-IS Well Known Ports page is displayed. [Table 8-6](#) lists all ports listed on the CDS-IS Well Known Ports page.

To view all ports in one page, from the **Rows** drop-down list, choose **All**.

**Table 8-6** Internet Streamer CDS-IS Well Known Ports

Source Group	Destination Group	Protocol	Source Port	Destination Port	Purpose
SE	SE	TCP	ANY	5274	Stream Scheduler
Administrator (PC)	CDSM	TCP	ANY	8443	Access CDSM GUI from Administrator PC
All Devices	NTP Servers	UDP	ANY	123	Query Time Servers
All Devices	NMS Servers	TCP	ANY	161	SNMP Query/Polling
All Devices	NMS Servers	UDP	ANY	162	SNMP/Trap
All Devices	Syslog Server	UDP	ANY	514	Syslog
All Devices	All Devices	TCP	ANY	22	SSH
All Devices	All Devices	TCP	ANY	23	Telnet (Disabled by default)
CDSM	SE	TCP	ANY	443	CDS Management (Notifications, updates, queries)
CDSM	SR	TCP	ANY	443	CDS Management (Notifications, updates, queries)
CDSM	CDSM	TCP	ANY	443	CDS Management (Notifications, updates, queries)
CDSM	CDSM	UDP	ANY	2000	CDSM to CDSM KeepAlives
DNS Server	All Devices	UDP	ANY	1023-65535	DNS Server responses to DNS query requests
DNS Server/Proxy	SR	UDP	ANY	53	DNS Query for RRFQDN from DNS Server/Proxy used by Subscriber(PC)
Origin Server	SE	TCP	ANY	1023-65535	Origin Server responses to HTTP requests
Origin Server	SE	UDP	ANY	1023-65535	Origin Server responses to RTSP requests
Origin Server	SE	TCP	ANY	ESTABLISHED PORT	Origin Server responses to SE to the port SE established the connection with the Origin Server
SE	CDSM	TCP	ANY	443	CDS Mgmt (Notifications, updates, queries)
SE	SE	TCP	ANY	443	Acquisition and Distribution
SE	SR	UDP	ANY	2323	Service Engine to Service Router KeepAlives
SE	CDSM	UDP	ANY	2000	Service Engine to CDSM KeepAlives
SE	SE	TCP	ANY	554	RTSP Requests between Service Engine
SE	SE	TCP	ANY	80	HTTP Request between Service Engine
SE	SE	TCP	ANY	5262	Metadata Receiver in Service Engine

**Table 8-6** Internet Streamer CDS-IS Well Known Ports (continued)

<b>Source Group</b>	<b>Destination Group</b>	<b>Protocol</b>	<b>Source Port</b>	<b>Destination Port</b>	<b>Purpose</b>
SE	SE	TCP	ANY	5275	Metadata Receiver in Service Engine
SE	SE	TCP	ANY	5263	Metadata Sender in Service Engine
SE	SE	TCP	ANY	5278	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 Streaming Live and Interactive Applications
SE	SE	TCP	ANY	80	Flash VOD file requests via http
SE	SE	TCP	ANY	550	Movie Streamer audio video transport
SE	Origin Server	TCP	ANY	80	Acquire Content from Origin Server using HTTP
SE	Origin Server	TCP	ANY	443	Acquire Content from Origin Server using HTTPS
SE	Origin Server	TCP	ANY	21	Acquire Content from Origin Servers using FTP
SE	Origin Server	TCP	ANY	139	Acquire Content from Origin Server using SMB
SE	Origin Server	TCP	ANY	80	Get Flash vod content from Origin Server by Acquire Content using HTTP
SE	Origin Server	TCP	ANY	1935	Get Flash live stream from Active acquirer or proxy interactive application data from edge SE to Origin Server using RTMP
SE	Origin Server	TCP	ANY	554	Acquire Content from Origin Server using RTSP
SE	NFS NAS Server	TCP	ANY	2049	Mounting NFS Shares
SE	SE	TCP	ANY	5266	Multicast Receiver in Service Engine
SE	SE	TCP	ANY	5267	Multicast Sender in Service Engine
SE	SE	TCP	ANY	5272	Primary/Backup Multicast Sender communication in Service Engine
SE	SE	TCP	ANY	5276	Multicast connectivity test tool sender request port in Service Engine
SE	SE	TCP	ANY	5277	Multicast connectivity test tool listener response port in Service Engine
SE	SE	TCP	ANY	4050	Multicast FXD Sender monitor port in Service Engine
SE	SE	TCP	ANY	4051	Multicast FXD Receiver monitor port in Service Engine
SE	SE	TCP	ANY	3057	Multicast FXD Sender PGM monitor port in Service Engine
SE	SE	TCP	ANY	3058	Multicast FXD Receiver PGM monitor port in Service Engine
SR	CDSM	TCP	ANY	443	CDS Mgmt (Notifications, updates, queries)
SR	CDSM	UDP	ANY	2000	Service Router to CDSM KeepAlives

**Table 8-6** Internet Streamer CDS-IS Well Known Ports (continued)

<b>Source Group</b>	<b>Destination Group</b>	<b>Protocol</b>	<b>Source Port</b>	<b>Destination Port</b>	<b>Purpose</b>
SR	SR	TCP	ANY	179	BGP communication Service Router
SR	SR(Proximity Engine mode)	TCP	ANY	7003	Proximity requests to SR (Proximity Engine) from SR  <b>Note</b> The SOAP API and associated port 7003 are only available when proximity-based routing is enabled on the SR.
SR	SR(Proximity Engine mode)	TCP	ANY	9000	SRP communication on Service Router Proximity Engine.
SR	SR(Proximity Engine mode)	UDP	ANY	9000	SRP communication on Service Router Proximity Engine.
SR	SR(Proximity Engine mode)	UDP	ANY	9003	SRP communication on Service Router Proximity Engine.
SR	SR(Proximity Engine mode)	UDP	ANY	9004	SRP communication on Service Router Proximity Engine.
SR	SR	TCP	ANY	9000	For SRP communication.
SR	SE	TCP	ANY	5283	Service Router-Service Engine RPC
Subscriber(PC)	DNS Server/Proxy	UDP	ANY	53	DNS Query for RRFQDN from Subscriber(PC)
Subscriber(PC)	SR	TCP	ANY	80	HTTP Request to Service Router from Subscriber(PC)
Subscriber(PC)	SR	TCP	ANY	80	RTMPT 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) 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	80	RTMPT 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) Request to Service Engine from Subscriber(PC)
Subscriber(PC)	SE	TCP	ANY	1755	MMS Request to Service Engine from Subscriber(PC)
Subscriber(PC)	SE	TCP	ANY	1111	Flash Media Server Administration

**Note**

The Destination Ports that have a port range indicate the possible ports that the Source Group could be expecting to send traffic to and receive traffic from. The specific ports required to be open to receive and send data depends on the Source Group configuration.

## Device Monitoring

This section covers the following topics:

- [Devices Table](#)
- [Devices Home Page](#)
- [Using show and clear Commands](#)
- [Core Dump Files](#)
- [CPU Utilization](#)

For more detailed statistics on HTTP, Web Media, Movie Streamer, and Flash Media Streaming traffic, see the “[Viewing Statistics](#)” section on page 8-44.

## Devices Table

The Devices Table page displays all devices registered in the VDS-IS network ([Figure 8-6](#)).

**Figure 8-6      Devices Table Page**

The screenshot shows the Cisco Content Delivery System Manager interface. At the top, there's a navigation bar with links for Home and Logout. Below that is a system status summary showing 3 devices and 2 services in critical condition. The main area is titled "Devices" and contains a table with the following columns: Device Name, Type, IP Address, Status, Location, and Software Version. The table lists 11 entries, with the last entry being Q6-CDE200-1. The bottom of the table shows page navigation (Page 1, 2, >>) and a total count of 11 devices.

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 8-7](#) 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 8-7** 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.
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. See the Server Offload field in <a href="#">Table 4-6 on page 4-11</a> for more information. 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 8-30 on page 8-45</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 the Software</a>” section on page 9-6.</li> <li>• Online [Waiting for data feed]—In some situations, the CDSM may receive regular heartbeat messages, but not receive a data feed message for a long time. The Online [Waiting for data feed] state indicates that the CDSM has not received a data feed message from this online device in the last 2.25 * polling rate seconds. When the data feed message is received, the state changes to Online.</li> </ul>
Location	Location the device is assigned to.
Software Version	Device software version.

**Table 8-8** 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 8-8** Device Table Icons

Icon	Function
	Create New device creates a Virtual Video Infrastructure Manager, Caching Node, or Library Node. <b>Note</b> The Create New Device pages are part of the integration with VDS-TV, which is an EFT feature.
	Activate all inactive Service Engines.
	Edit the device.
	Export a table to a comma-separated value (CSV) file.

**Table 8-8** Device Table Icons (continued)

Icon	Function
	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.

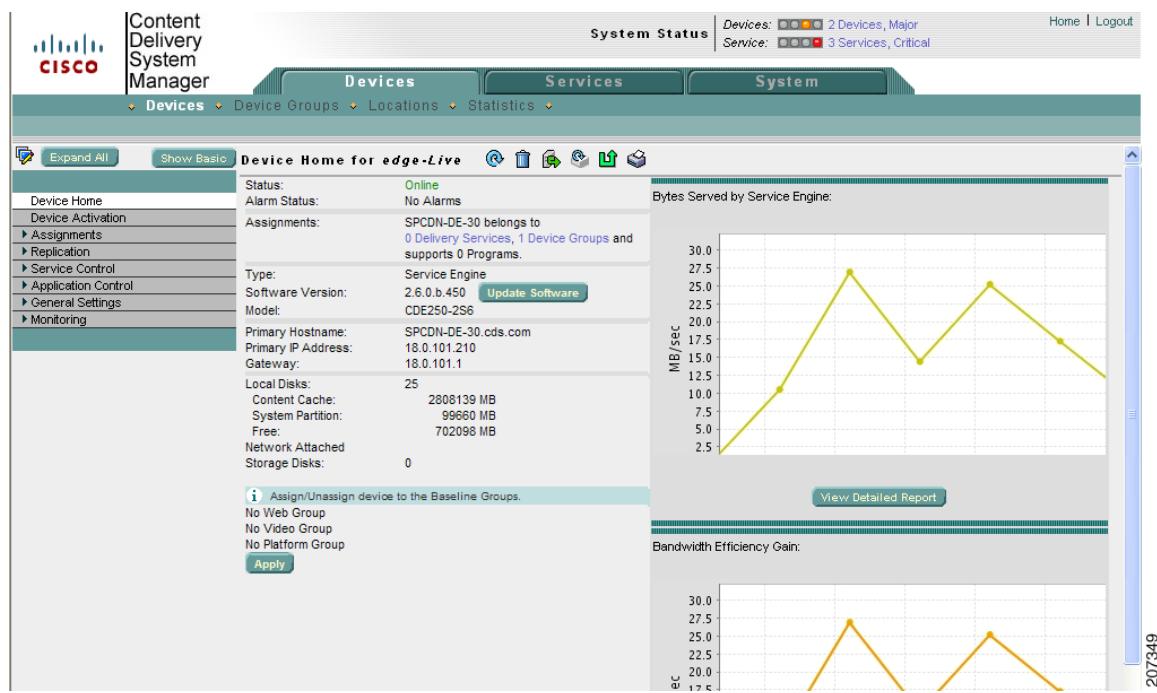
For more information, see the “Devices, Services, and Other Tables” section on page 3-7.

## Devices Home Page

The Devices home page ([Figure 8-7](#)) 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 VDS-IS, 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, and telnet to the device from the Devices home page. For more information about updating the software, see the “Software Upgrade” section on page 9-1.

**Figure 8-7 SE Devices Home Page**

The Bandwidth Served by Service Engine and the Bandwidth Efficiency Gain graphs are also displayed. For more information, see the “Reports” section on page 8-26.

The Devices home page for an SE or an SR provides several icons. Table 8-9 describes these icons. The CDSM home page has a subset of the icons.

**Table 8-9 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 “Deleting a Device” section on page 9-10.
	Updates application statistics. The device statistics are updated at a configurable time interval, which is set in the System Configuration page (System.monitoring.collectRate). See the “Configuring System Settings” section on page 6-8. To see the latest statistics immediately, without waiting for the time interval to elapse, click this icon.

**Table 8-9 SE Devices Home Page Icons (continued)**

Icon	Description
	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 9-10.
	Prints the home page.

For more information about the Devices home page, see the “[Devices Home Page](#)” section on page 3-8. For more information on activating Devices via Device home page, see the “[Activating and Setting NTP for Each Device](#)” section on page 3-3.

## Using show and clear Commands

The **show** and **clear** commands offer more detailed monitoring of the device. [Table 8-10](#) lists only the **show** command parameters where arguments are required or are optional. [Table 8-11](#) lists only the **clear** command parameters where arguments are required. A full list of the **show** and **clear** commands is available from the drop-down list on the respective page.

### Using the CDSM show or clear Command Tool

To use the CDSM show or clear command tool, follow these steps:

- 
- Step 1** Choose **Devices > Devices > Monitoring > Show/Clear Commands** and then click either **Show Commands** or **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.
- 

**Table 8-10 show Command Arguments**

show Command	Arguments	Device
aaa	{ commands [accounting   authorization]   enable [authentication]   exec [accounting   authorization]   login [authentication]   system [accounting   authorization] }	SE, SR, CDSM
access-list	{300}	SE

**Table 8-10** show Command Arguments (continued)

show Command	Arguments	Device
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
alarms	[ <b>critical</b>   <b>detail</b>   <b>history</b>   <b>major</b>   <b>minor</b>   <b>status</b> ]	SE, SR, CDSM
authentication	{ <b>user</b> }	SE, SR, CDSM
authsvr	[ <b>location-server</b>   <b>unknown-server</b> ]	SE
bandwidth	[ <b>flash-media-streaming</b>   <b>movieStreamer</b>   <b>wmt</b> ]	SE
bitrate	[ <b>wmt</b>   <b>movieStreamer</b> ]	SE
cache	[ <b>content</b> <i>1-1000</i> ]	SE
cache-router	{ <b>routes</b> { <b>dss-engine</b>   <b>fms-engine</b>   <b>web-engine</b>   <b>wmt-engine</b> }   <b>upstream-status</b> }	SE
capability	{ <b>profile</b> <i>1-65535</i> }	SE
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
cdnfs	{ <b>usage</b>   <b>volumes</b> }	SE
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
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
content	{ <b>all</b>   <b>diskpath</b> <i>diskpath</i>   <b>last-folder-url</b> <i>url</i>   <b>url</b> <i>url</i> }	SE
content-mgr	{ <b>content</b> { <b>all</b> { <b>all-disk-volumes</b> <b>output-file</b> <i>filename</i>   <b>disk-volume</b> <i>disk_num</i> <b>output-file</b> <i>filename</i> }   <b>cache</b> { <b>all-disk-volumes</b> <b>output-file</b> <i>filename</i> }   <b>disk-volume</b> <i>disk_num</i> <b>output-file</b> <i>filename</i> }   <b>prepos</b> { <b>all-disk-volumes</b> <b>output-file</b> <i>filename</i> }   <b>disk-volume</b> <i>disk_num</i> <b>output-file</b> <i>filename</i> }   <b>disk-info</b>   <b>eviction-list</b> <b>size</b> <i>file_size</i> { <b>all-disk-volumes</b> <b>output-file</b> <i>filename</i> }   <b>disk-volume</b> <i>disk_num</i> <b>output-file</b> <i>filename</i> }   <b>eviction-protection</b> <b>output-file</b> <i>filename</i>   <b>health-info</b> }	SE
content-origin	[ <b>request-fqdn</b> <i>domain_name</i> ]	SE
device-mode	{ <b>configured</b>   <b>current</b> }	SE, SR, CDSM
disks	[ <b>current</b>   <b>details</b>   <b>error-handling</b> [{ <b>details</b> }]   <b>raid-state</b>   <b>SMART-info</b> [{ <b>details</b> }]]	SE, SR, CDSM

**Table 8-10** show Command Arguments (continued)

show Command	Arguments	Device
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> ]] [ <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> ]]] [ <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> ]] [ <b>object-status</b> <i>object-url</i> ] [ <b>processes</b>   <b>remote</b> ] [ <b>remote ip-address</b> { <b>metadata-sender 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 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>remote traceroute</b> { <b>forwarder-next-hop 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 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
flash-media-streaming	[ <b>logging</b> <i>filename</i> ]   <b>stream-status</b> <b>live</b> [all <i>filename</i> ]]	SE, SR
interface	{ <b>GigabitEthernet</b> <i>slot/port</i>   <b>PortChannel</b> <i>port-num</i>   <b>Standby</b> <i>group_num</i>   <b>TenGigabitEthernet</b> <i>slot/port</i> }	SE, SR, CDSM

**Table 8-10** show Command Arguments (continued)

show Command	Arguments	Device
ip	On SE or CDSM: {access-list [acl-name   acl-num]   routes} On SR: {access-list [acl-name   acl-num]   bgp {ip-prefix   network-ip-address   all   community [location-community]   ipv4 unicast   memory   neighbors [neighbor-ip-address]   nexthop-database   summary}   interface brief   ospf [border-routers   database [adv-router ip-address-advertising-router   asbr-summary   ip-address-link-state-id   detail]   database-summary   detail   external [ip-address-link-state-id   detail]   network [ip-address-link-state-id   detail]   nssa-external   ip-address-link-state-id   detail]   router [ip-address-link-state-id   detail]   self-originated [detail]   summary [ip-address-link-state-id   detail]]   interface   memory   neighbor [ip-address-neighbor [detail]   detail   summary]   request-list ip-address-neighbor-router {GigabitEthernet slot/port   PortChannel channel-number}   retransmission-list {GigabitEthernet slot/port   PortChannel channel-number}   route [single-ip-route]   rsvp route [ip-address-advertising-router]   traffic   proximity {algorithm   server}   rib {clients [single-client]   memory   recursive-next-hop [ip-address-next-virtual-hop]   route [ip-address-single-route]   bgp   direct   isis   ospf   summary]   unresolved-next-hop [ip-address-unresolved-next-hop]}   route   static route}	SE, SR, CDSM
IPv6	access-list [1-99 standard IPv6   100-199 extended IPv6   access_list_name]   routes	SE, SR, CDSM
isis	adjacency [detail]   clns route   database [advertise   detail [lsp id]   private   summary   lsp-id]   hostname-table   interface [GigabitEthernet slot/port   PortChannel channel-number]   ip {route [ip-address-route [detail]   detail   summary]   rsvp route [lsp-id]   memory   process   rrm {GigabitEthernet slot/port   PortChannel channel-number}   spf-log [detail]   srm {GigabitEthernet slot/port   PortChannel channel-number}   ssn {GigabitEthernet slot/port   PortChannel channel-number}}	SR
key	{chain [decrypt   keychain-name]}	SR
lacp	{counters   internal}	SE, SR, CDSM
movie-streamer	[bandwidth   cache   proxy]	SE
ntp	{status}	SE, SR, CDSM
processes	[cpu   debug pid   memory   system [delay 1-60   count 1-100]]	SE, SR, CDSM
programs	[movie-streamer [cli   live   rebroadcast]   program-id program-id   program-name program-name   wmt [cli   live   rebroadcast]	SE

**Table 8-10** show Command Arguments (continued)

show Command	Arguments	Device
rtsp	{gateway}	SE
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}]   protocol {http   rtmp   rtsp}]   validate-url-signature [protocol {http   rtmp   rtsp}]]]   all   pattern-list {1-512 pattern-type   all}}	SE
service-registry	{process   service}	SR
service-router	On SE: {keepalive-interval   service-monitor} On SR: {access-policy   content-based-routing   forwarding [content-origin content-origin]   lastresort [domain domain-name]   load {all   sename sename}   location-based-routing   memory   proximity-based-routing   redirect-burst-control   redirect-mode   routes [content-origin content-origin]   service-monitor   services {all   sename sename}   subscribe domain   summary [content-origin content-origin]} } On CDSM: {service-monitor}	SE, SR, CDSM
services	{ports [port-num]   summary}	SE, SR, CDSM
snmp	{alarm-history   engine ID   group   stats   user}	SE, SR, CDSM
srp	{database {key-hex-string   brief   content   group   maincontent target-string   record key-hex-string   service   size low high   statistics   subid key-hex-string target-string   update start end}   leafset   memory   multicast database [brief   statistics   group-id [elements start end   message target-string   sender key-hex-string]   neighbor [detail   down]   process   replica-set [statistics]   route [backup   statistics]   subscribers]}	
statistics	On all devices: aaa   fd   icmp   ip   lsof   netstat   radius   services   snmp   tacacs   tcp   udp On SR only: {cdn-select summary   ip [ospf   proximity {rib   server}]   isis [GigabitEthernet slot/port   PortChannel channel-number]   proximity-engine all   service-registry   service-router {all   content-origin content-origin   dns   history   keepalive   routing [geo-location   proximity] se se-name   summary} srp}	SE, SR, CDSM

**Table 8-10** show Command Arguments (continued)

show Command	Arguments	Device
statistics	<p>On CDSM only: <b>content-distribution-network device status</b>  <i>device-name</i> or <b>device-group-name</b> or <b>device-ID</b></p> <p><b>replication {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>}  <b>access-lists 300</b>  <b>acquirer [contents {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>}]  <b>authsvr [delivery-service-id</b> <i>delivery-service-num</i>   <b>global</b>]    <b>cdnfs</b>   <b>content-mgr</b>  <b>distribution {all   errors {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<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>flash-media-streaming [connections   dvrcast   errors  </b>  <b>flvcache   livestats   performance   proxy   rules   server   swf   vod]</b>  <b>movieStreamer {all   bw-usage   errors   performance  </b>  <b>requests   rule}</b>  <b>replication {content-items</b> <i>content-item</i>   <b>delivery-service</b>  [<b>selected-delivery-service</b> <i>content-origin-name</i>]}  <b>transaction-logs</b></b></p>	SE, SR, CDSM

**Table 8-10** show Command Arguments (continued)

show Command	Arguments	Device
statistics	web-engine [abr {hls-media-app [detail   fragment-file   manifest-file   session   summary]   smoothhd-media-app [detail   fragment-file   manifest-file   meta-file   session   summary]   zeri-media-app [detail   fragment-file   manifest-file   meta-file   summary]}   detail   error summary   key-client   performance   usage] wmt {all   bytes {incoming   outgoing}   cache   errors   multicast multicast-station   requests   rule   savings   streamstat [incoming   live   outgoing   stream-id 1-999999]   usage}	SE, SR, CDSM
tech-support	[list-files list-file-directory   page   service {acquisition-distribution   authentication   cms   flash-media-streaming   kernel   movie-streamer   rules   web-engine   wmt}]	SE, SR, CDSM
user	{uid number   username name}	SE, SR, CDSM
users	{administrative}	SE, SR, CDSM
version	[pending]	SE, SR, CDSM
web-engine	{all   delivery-service-configuration   health}	SE
wmt	[bandwidth [incoming bypass-list]   detail   diagnostics {header-info {nsc-file nsc-file   stream-file stream-file}   network-trace tcpdump-file}   http allow extension   proxy]	SE

**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.

**Table 8-11** clear Command Arguments

clear Command	Arguments	Device
cache	{all   content 1-15000   flash-media-streaming}	SE
content	{last-folder-url url   url url}	SE
isis	adjacency {all   GigabitEthernet slot/port   PortChannel channel-number}   ip rsvp route [lsp-id]	SR
ip	On all devices: {access-list counters 1-99 (standard IP) or 100-199 (extended IP) or access-list-name} On SR only: bgp {neighbor-ip-address   all}   ospf {neighbor {all   GigabitEthernet slot/port   PortChannel channel-number}   rsvp route [ip-address-advertising-router   traffic]}	SE, SR, CDSM

**Table 8-11** clear Command Arguments (continued)

clear Command	Arguments	Device
IPv6	<b>access-list counters</b> [1-99 standard IPv6   100-199 extended IPv6   <i>access_list_name</i> ]	SE, SR, CDSM
service-router	{ <b>proximity-based-routing proximity-cache</b> }	SR
srp	<b>database offline</b>   <b>descriptor</b> { <b>all</b>   <b>key-hex-string</b> }   <b>group</b> <b>messages</b>   <b>neighbor</b> { <b>key-hex-string</b>   <b>hostname:port</b> }   <b>resource</b> <b>key-hex-string unicast_resource</b>   <b>route</b> <b>prefix/length</b>	
statistics	On all devices: <b>aaa</b>   <b>all</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> 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> } On SR only: <b>http requests</b>   <b>ip</b> [ <b>ospf</b>   <b>proximity</b> [ <b>rib</b>   <b>server</b> ]]]   <b>isis</b> [ <b>GigabitEthernet slot/port</b>   <b>PortChannel channel-number</b> ]   <b>service-registry</b>   <b>service-router</b>   <b>srp</b> [ <b>replica-set</b> ] On SE only: { <b>access-lists 300</b>   <b>authsvr</b> { <b>all</b>   <b>delivery-service-id</b> <b>delivery-service-num</b>   <b>global</b> }   <b>content-mgr</b>   <b>flash-media-streaming</b>   <b>movie-streamer</b>   <b>qos 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> { <b>1-512</b>   <b>all</b> }   <b>rtsp</b> }   <b>transaction-logs</b>   <b>web-engine</b> [ <b>force</b> ]   <b>wmt</b> }	SE, SR, CDSM
users	{ <b>administrative</b> }	SE, SR, CDSM
wmt	{ <b>encoder-alarm-msg</b> <i>alarm-message</i>   <b>stream-id</b> 1-999999   <b>[stale-stat]</b> }	SE



**Note** The **clear statistics web-engine** and **clear statistics all** commands only clear normal statistics, not the Web Engine statistics details. To clear all Web Engine statistics, use the **clear statistics web-engine force** command. We do not recommend using the **clear statistics web-engine force** command, but if it is used, restart the Web Engine service by entering the **web-engine stop** and **web-engine start** commands.

## Core Dump Files

The Core Dump Files page lists any core dump files for the device. To view a list of core dump files for the device, choose **Devices > Devices > Monitoring > Core Dump Files**. The Core Dump File page is displayed and lists any core dump files that have occurred on the device.

To delete a core dump file, check the check box next to the filename and click the **Delete** icon in the task bar.

To delete all core dump files, check the check box in the heading of the check box column, and click the **Delete** icon in the task bar.

To refresh the table, click the **Refresh Table** icon in the task bar.

To print the table, click the **Print** icon in the task bar.

The core dump files are located in the **/local/local1/core\_dir** directory.

## CPU Utilization

The CPU Utilization report displays the CPU usage for the SE.

To view the CPU Utilization report for an SE, follow these steps:

- 
- Step 1** Choose **Devices > Devices > Monitoring > Statistics > CPU Utilization**. The CPU Utilization Report page is displayed.
- Step 2** Enter the settings as appropriate. [Table 8-12](#) describes the report settings.

**Table 8-12 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. There is a difference in the meaning of the graphs based on the time frame chosen: <ul style="list-style-type: none"><li>• Last Hour—Shows raw data collected from the SEs. Real-time values are reported.</li><li>• Last Day—Shows hourly data, which consolidates the raw data. Consolidation is done by averaging the raw data for each hour. So the value reported in the Last Day graph are average values per hour.</li><li>• Last Week, Last Month, and Custom—Shows daily data, which consolidates hourly data. Consolidation is done by averaging the hourly data for each day. So these are average values per day.</li></ul>
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.
- 

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.

# Reports

There are three reports available for monitoring traffic in graphical or tabular format:

- [Bandwidth Served](#)
- [Bandwidth Efficiency Gain](#)
- [Streaming Sessions](#)

The reports have the following three scopes:

- System-wide
- Location
- Service Engine

To access the system-wide reports, click the **Home** link in the upper-right corner of the CDSM browser window. To change the report parameters for the System-Wide Bandwidth Served or System-Wide Bandwidth Efficiency Gain graphs, click **View Detailed Report**. Clicking the **Streaming Sessions** link opens 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 6-8



**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 4-64 for more information.

To access reports covering activity for a location, follow these steps:

- 
- 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**.
- 

To access reports covering activity for an SE, follow these steps:

- 
- 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**, or **Streaming Sessions**.

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.

The reports are described in the following sections.

## 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 VDS-IS 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 “[Reports](#)” section on page 8-26.

[Table 8-13](#) describes the report settings.

**Table 8-13 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.

**Table 8-13 Bandwidth Served Report Settings (continued)**

Field	Description
Time Frame	The time frame options are last hour, last day, last week, last month, or custom. There is a difference in the meaning of the graphs based on the time frame chosen: <ul style="list-style-type: none"> <li>• Last Hour—Shows raw data collected from the SEs. Real-time values are reported.</li> <li>• Last Day—Shows hourly data, which consolidates the raw data. Consolidation is done by averaging the raw data for each hour. So the value reported in the Last Day graph are average values per hour.</li> <li>• Last Week, Last Month, and Custom—Shows daily data, which consolidates hourly data. Consolidation is done by averaging the hourly data for each day. So these are average values per day.</li> </ul>
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 8-14](#) describes the report settings.

**Table 8-14 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 8-14 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. There is a difference in the meaning of the graphs based on the time frame chosen: <ul style="list-style-type: none"> <li>• Last Hour—Shows raw data collected from the SEs. Real-time values are reported.</li> <li>• Last Day—Shows hourly data, which consolidates the raw data. Consolidation is done by averaging the raw data for each hour. So the value reported in the Last Day graph are average values per hour.</li> <li>• Last Week, Last Month, and Custom—Shows daily data, which consolidates hourly data. Consolidation is done by averaging the hourly data for each day. So these are average values per day.</li> </ul>
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 8-15](#) describes the report settings.

**Table 8-15 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.
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.

**Table 8-15 Streaming Sessions Report Settings (continued)**

Field	Description
Time Frame	The time frame options are last hour, last day, last week, last month, or custom. There is a difference in the meaning of the graphs based on the time frame chosen: <ul style="list-style-type: none"> <li>• Last Hour—Shows raw data collected from the SEs. Real-time values are reported.</li> <li>• Last Day—Shows hourly data, which consolidates the raw data. Consolidation is done by averaging the raw data for each hour. So the value reported in the Last Day graph are average values per hour.</li> <li>• Last Week, Last Month, and Custom—Shows daily data, which consolidates hourly data. Consolidation is done by averaging the hourly data for each day. So these are average values per day.</li> </ul>
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, VDS-IS 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.

**Tip**

Set the Chart Size to medium to see the legend and timeline across the bottom.

## Delivery Service Monitoring

This section covers the following topics:

- [Delivery Services Table, page 8-30](#)
- [Processing Content Deletion, page 8-34](#)[Content Deletion Tasks, page 8-35](#)
- [Replication Status for a Delivery Service, page 8-37](#)

## 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 8-16** 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 8-16 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 page.
	Deletes a Single URL or Multiple content URL.

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, follow these steps:

- 
- Step 1** Choose Services > Delivery Services to display the Delivery Services Table page. See [Figure 8-8](#).

**Figure 8-8 Delivery Services Table Page**

The screenshot shows the Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Software Configuration Guide. The top navigation bar includes 'Content Delivery System Manager', 'System Status' (Devices: 4 Devices, Critical; Service: 1 Service, Critical), 'Home | Logout', and tabs for 'Devices', 'Services', and 'System'. Below the tabs is a sub-navigation bar with 'Service Definition' (selected), 'Live Video', 'Delivery Services' (selected), and 'Content Origins'. The main content area is titled 'Delivery Services' and contains a table with the following data:

Delivery Service	Type	Content Origin	Status	State	Manifest State
100kbps	Content	100kbpsfiles		N/A	N/A
1mb	Content	1mb		N/A	N/A
1mb100	Content	1mb100file		N/A	N/A
375mb100wmv	Content	375mbps100files		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
8kdfile	Content	8kfiles		N/A	N/A
8kbs	Content	8kb		N/A	No Status Reported
8lfiles	Content	8lfiles		N/A	N/A

At the bottom of the table, it says 'Showing 1-10 of 30 Delivery Services'.

- Step 2** View the replication status information for each Delivery Service. [Table 8-17](#) describes the status information that is displayed on this page.

**Table 8-17 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 8-18</a> for a description of status errors and their corresponding status lights.)</p>
State	<p>State of the Delivery Service. States are reported for the Content Acquirer and for receiver SEs. (See <a href="#">Table 8-19</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 8-10</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 8-18](#) describes the status errors and their corresponding status lights.

**Table 8-18 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.

**Table 8-18 Delivery Service Status Errors (continued)**

Status Light	Error	Description
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 8-19 defines the different Delivery Service states.

**Table 8-19 Delivery Service States in Replication Status**

State	Description
Completed	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 8-25 on page 8-39</a> for a description of SE states.) 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.
In Process	In Process can mean: <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	Failed can mean: <ul style="list-style-type: none"> <li>• Acquisition or content replication error has occurred. (See <a href="#">Table 8-18 on page 8-32</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>

## Processing Content Deletion

Starting from Release 3.3, VDS-IS supports content deletion per Delivery Service and per Service Engine by using wildcards. To remove the cached content in SEs, you need to request for a content deletion task from the CLI, or the CDSM GUI, or using the API.



- Note** You do not have to manually delete the contents for a non-existing Delivery Service or content origin.

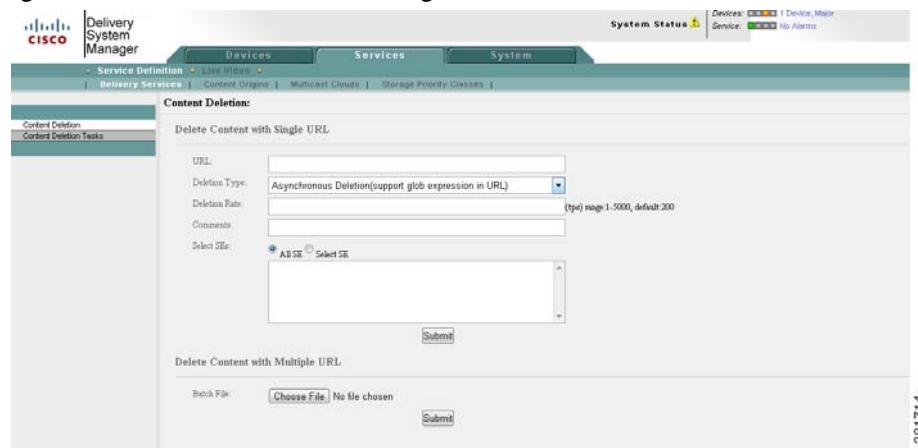
To delete the content in the SE, follow these steps:

**Step 1** Choose Services > Service Definition. The Service Definition page is displayed.

**Step 2** Click the **Process Content Deletion** icon in the task bar. The Content Deletion page is displayed

[Figure 8-9](#)

**Figure 8-9 Content Deletion Page**



**Step 3** There are 2 modes to delete the content.

- **Delete Content with Single URL**—Delete content of a single URL.
- **Delete Content with Multiple URL**—Delete content of multiple URLs.

**Step 4** If you choose to delete the content with single URL, enter the settings as appropriate in the **Delete Content with Single URL** pane.

- In the **URL** field, enter the URL to delete.



- Note** For the IPv6 URLs, the URL should be of this form : `http://xx:xx::xx/test.mp4`. Do not include the TCP port as a part of the URL.

- From the **Deletion Type** drop-box, choose one of the following:
  - **Asynchronous Deletion** -Supports Global expressions in the URL.
  - **Synchronous Deletion** - Does not support Global expressions in the URL.
- In the **Deletion Rate** field, enter the number of files to be deleted per second in a Service Engine. The range is from 1 to 5000. The default deletion rate is 200.

- In the **Comments** field, enter the user comments if any.
- Step 5** If you choose the **Delete Content with Multiple URL** pane, click **Choose File**, to locate the XML file and upload the XML file.  
For more information on viewing or downloading the XML file, see [Viewing or Downloading XML Schema Files, page 6-24](#)
- Step 6** Click **Submit**.
- 

## Content Deletion Tasks

The content deletion tasks page provides the status of deletion in the service engine, and the status of a specific URL deletion per service engine. A completed task can be deleted using the CDSM GUI, the API, or the CLI.



**Note** Only after the tasks are completed, you can delete the tasks.

The deletion tasks are created in the back-end and are long-running tasks.

- Cancel Running Tasks—A deletion task is always dispatched to multiple SEs. If all the contents of a specific URL is deleted successfully while the SE receives the canceling request, the deletion status for the URL is **File Delete Success**. If some contents fail in deleting while the others deleted successfully, the status is **File Delete Failure**. If some content deletion is canceled successfully, the status is **Deletion Canceled**.
- Delete Completed task—A completed task can be deleted using the CDSM GUI, the API, or the CLI.

[Table 8-20](#) describes the content deletion task status.

**Table 8-20 Content Deletion Task Status**

Code	Status	Description
0	Created	This status appears when the task is created in Database, but is not sent to any SE.
1	Deleting	This status appears when the deletion is in process.
2	Content Deleted	This status appears when the deletion is success for all SE.
3	Content Delete Failed	This status appears when the deletion failed. If the deletion fails for any SE, the status will reflect as content delete failed.
4	Canceling	This status appears when the deletion task is being canceled.
5	Canceled	This status appears when the deletion task is canceled successfully.
6	Cancel Failed	This status appears when, canceling failed.

[Table 8-21](#) describes task status of SE.

**Table 8-21 Task Status of SE**

<b>Code</b>	<b>Status</b>	<b>Description</b>
0	Created	This status appears when the task is created in DB, but has not started deleting.
1	Content Deleting	This status appears when the deletion in process.
2	Content Deleted	This status appears when the SE completes the deletion task.
3	Content Delete Failed	This status appears for one of the following reasons: <ul style="list-style-type: none"> <li>• Task is failed to be sent to SE</li> <li>• There exists deletion failure for a URL</li> </ul>
4	Canceling	This status appears when the deletion task is being canceled in the SE.
5	Canceled	This status appears when the deletion task is canceled successfully.
6	Cancel Failed	This status appears when, canceling was not successful.
7	Terminated Exceptionally	This status appears when the task is in CDSM but not exist in SE.
8	Delete Timeout	This status appears when, deletion task has not been updated for a long time.
9	Cancel Timeout	This status appears when, canceling deletion task has not been updated for a long time.

Table 8-22 describes the URL status of SE.

**Table 8-22 URL Status of SE**

<b>Code</b>	<b>Status</b>	<b>Description</b>
0	Created	This status appears when the URL is created in DB, but has not start deleting.
6	File NOT Found	This status appears when no file is found for the URL
17	File Delete Success	This status appears when the files are deleted successfully.
19	Pending For Deletion	This status appears when the URL is pending for deletion.
20	File Deleting	This status appears when files are being deleting.
21	File Delete Failure	This status appears when any error happens while deleting is in process
23	Deletion Canceling	This status appears when the deletion for the URL is being canceled.
24	Deletion Canceled	This status appears when, canceling for the URL was not successful.
901	Terminated Exceptionally	This status appears when the task is in CDSM but does not exist in SE.

## 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. Figure 8-10 shows the Replication Status page for a Delivery Service. The Replication Status page is refreshed automatically every 15 seconds.

**Figure 8-10** *Delivery Service Replication Status Page*

The screenshot shows the 'Content Delivery System Manager' interface. In the top right, there are status indicators: Devices (1 Device, Critical), Service (No Alarms), and Licenses (1 License, Critical). The main navigation bar includes 'Devices', 'Services', and 'System'. Below the navigation, a sub-menu for 'Service Definition' shows 'Live Video' selected. Under 'Delivery Services', 'fms' is selected. The main content area is titled 'Replication Status for Delivery Service, fms'. It contains sections for '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) and 'View Detailed Replication Status' (with a search bar). Below these is a table titled 'Devices Assigned to Delivery Service, fms' with columns for Device, Type, Status, State, Progress(in %), Last Report Time, and File Count (Completed, In Process, Failed). The table lists three devices: GE-612-2 (Acquirer, Completed, 100.00%, 16:36:44 05-05-2009, 7 files); GE-612-6 (Receiver, Completed, 100.00%, 16:36:50 05-05-2009, 7 files); and GE-612-7 (Receiver, Completed, 100.00%, 16:36:33 05-05-2009, 7 files). Navigation links at the bottom include '<< Page 1 >>' and 'Showing 1'.

Table 8-23 describes the fields in Acquisition Status section of this page.

This page also allows you to follow these steps:

- See a detailed view of replication status using search criteria. (See the “Content Replication Status by Delivery Service” section on page 8-40.)
- 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 8-42.)

The information on the Replication Status page is refreshed approximately every ten seconds.

**Table 8-23** *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.

**Table 8-23 Replication Status for a Delivery Service (continued)**

Field	Description
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 8-25</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 8-24](#) describes the information about the devices in this Delivery Service shown at the bottom of the Replication Status page.

**Table 8-24 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 8-25</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 6-8</a> ).
Last Report Time	Time when the last report from the SE was received by the CDSM. This time stamp uses the CDSM clock.
File Count	
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.

**Table 8-24 Replication Status for Devices Assigned to a Delivery Service (continued)**

Field	Description
Failed	For the Content Acquirer: Number of files that failed to be acquired in at least one attempt. For receiver SEs: Number of files that failed to be replicated in at least one attempt. <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 8-25 describes the states of the Content Acquirer or receiver SE.

**Table 8-25 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.
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.

**Table 8-25 Device States (continued)**

State	Description
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**.

For help on allowed 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 8-11 shows the results of a detailed status search for a Delivery Service.

**Figure 8-11 Replication Status for Searched Content Items in a Delivery Service**

The screenshot shows the Cisco Content Delivery System Manager interface. The top navigation bar includes links for Home, Logout, System Status (Devices: 1 Device, Critical; Service: 2 Services, Critical), and tabs for Devices, Services, and System. A sub-navigation bar under 'Service Definition' shows 'Live Video' and 'Delivery Services' (which is selected). On the left, a sidebar lists options like Definition, Delivery Service Content, PCMM Config, General Settings, Assign Service Engines, List all assigned Service Engines, Replication Status, and Tools. The main content area is titled 'Replication Items - Delivery Service: rev-prep-sr'. It displays a table with columns: Url, Size, Status, Replied SEs, Playtime, and Modification Time. Three items are listed:

Url	Size	Status	Replied SEs	Playtime	Modification Time
http://3.1.14.13/548kbs.wmv	10.014 MB	Pending	3	00:02:52	10:32:41 03-22-2007
http://3.1.14.13/multi.aspx	107 Bytes	Pending	3	-	12:44:16 07-13-2007
http://3.1.14.13//MLoad.asp	49.860 KB	Pending	3	00:00:21	07:10:29 03-22-2007

Page navigation at the bottom indicates '<< Page 1 >>' and 'Showing 1-3 of 3 Content Items'.

Table 8-26 describes the information displayed for the replication items.

**Table 8-26 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.

**Table 8-26 Replication Status of Items for a Delivery Service**

Column Heading	Description
Replicated 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 8-12). This page provides details on the replication status of the content item for every SE in the Delivery Service.

Table 8-27 describes the information on this page.

**Figure 8-12 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 8-27 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.

**Table 8-27 Replication Status of an Item for All SEs in a Delivery Service**

Column Heading	Description
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, follow these steps:

- 
- Step 1** From the Replication Status page, in the Devices Assigned to Delivery Service section (see [Figure 8-10](#)), 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, follow these steps:
- Choose content items (**all**, **replicated**, or **nonreplicated**) from the **Get** drop-down list.
  - 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 ([Figure 8-13](#)). [Table 8-28](#) describes the fields displayed in this page.

**Figure 8-13 Replication Items for a Selected Device**

The screenshot shows the Cisco Content Delivery System Manager interface. At the top, there's a navigation bar with the Cisco logo, 'Content Delivery System Manager', 'System Status' (Devices: 1 Device, Critical; Service: 2 Services, Critical), 'Home | Logout', and tabs for 'Devices', 'Services', and 'System'. Below the navigation bar is a sub-navigation menu with 'Service Definition' (selected), 'Live Video', 'Delivery Services' (selected), and 'Content Origins'. A search bar at the top right says 'Replication Items - Delivery Service: rev-prep-sr Service Engine: CC-612-4' with a refresh icon and a 'Go' button. To the right of the search bar is a dropdown for 'Rows' set to 10. The main content area is titled 'Replication Items - Delivery Service: rev-prep-sr Service Engine: CC-612-4' and shows a table of replication items. The table has columns: Url, Size, Status, Playtime, and Modification Time. The data in the table is:

Url	Size	Status	Playtime	Modification Time
http://3.1.14.13/548kbs.wmv	10.014 MB	Complete	00:02:52	10:32:41 03-22-2007
http://3.1.14.13/multi.aspx	107 Bytes	Complete	-	12:44:16 07-13-2007
http://3.1.14.13/WMLoad.asf	49.880 KB	Complete	00:00:21	07:10:29 03-22-2007

At the bottom left is a 'Page 1' link, and at the bottom right it says 'Showing 1-3 of 3 Content Items'. A small number '211829' is in the bottom right corner.

**Table 8-28 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, follow these steps:

- Make a choice from the **Get** drop-down list.
- Enter a search string in the **Content Items Using** field.
- To retrieve the specified items, click **Go**.

**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 VDS-IS. 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 VDS-IS, and provides a drill-down to all delivery services for a chosen SE, and all content items associated with that Delivery Service. The Proximity Engine statistics provides overall statistical information on the Proximity Engine, and specific statistical information on IS-IS, OSPF, and SRP.

This section contains the following procedures:

- [Viewing Service Engines and Device Group Statistics](#)
- [Viewing Routing Statistics](#)
- [Viewing Replication States](#)
- [Viewing Proximity Engine Statistics](#)

## Viewing Service Engines and Device Group Statistics

To view the statistics for all SEs or all device groups, follow these steps:

- 
- 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 8-29](#) describes the icons provided on the Statistics pages.

**Table 8-29 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 “Configuring System Settings” section on <a href="#">page 6-8</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 8-30](#) describes each statistic for each content delivery type.

**Table 8-30 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 Statistics**

## Viewing Routing Statistics

To view the routing statistics for SRs, follow these steps:

---

**Step 1** Choose **Devices > Statistics > Routing Statistics**.

**Step 2** Choose one of the following options:

- **Routing Requests**
- **Routing Redirects**

See [Table 8-29](#) for descriptions of the icons provided on the Routing Statistics pages. [Table 8-31](#) describes each routing statistic.

**Table 8-31 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, follow these steps:

---

**Step 1** Choose **Devices > Statistics > Replication Status**. The replication states for all SEs in the VDS-IS are displayed.

[Table 8-32](#) describes the status information displayed on this page.

**Table 8-32 Device Replication Status Page**

<b>Column Heading</b>	<b>Description</b>
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 8-18</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 8-25</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 8-24 on page 8-38](#).
- 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**, or **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 8-33](#) 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 8-33 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.

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.

## Viewing Proximity Engine Statistics

This section contains the following procedures:

- [Viewing Overall Proximity Statistics](#)
- [Viewing IS-IS Statistics](#)
- [Viewing OSPF Statistics](#)
- [Viewing SRP Statistics](#)

See [Table 8-29](#) for descriptions of the icons provided on the Proximity Statistics pages.

## Viewing Overall Proximity Statistics

To view the overall statistics of the Proximity Engine, follow these steps:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the Service Router. The Devices home page is displayed.
  - Step 3** Choose **Statistics > Proximity**. The Proximity Statistics are displayed.

[Table 8-34](#) describes each proximity statistic.

**Table 8-34 Proximity Statistics**

Statistic	Description
Application total requests	Total number of proximity requests received from applications.
Application total replies	Total number of proximity replies sent to applications.
Invalid Application request	Invalid proximity requests from applications.
PSA non-rankable application requests	Proximity source address (PSA) non-rankable proximity requests from applications.
Failed proximity requests	Failed proximity requests to routing protocols.
Failed PSA lookups	Failed PSA lookups.
Failed PTA lookups	Failed proximity target address (PTA) lookups.
Location Application requests	Local proximity requests from applications.
Message	Routing protocol participating in message exchange.
Sent Prox Req	Proximity message exchanges between the routing process and the routing protocols.
Received Prox Req	Proximity message exchanges between the routing process and the routing protocols.
Proximity Server Requests Received	Received requests by the Proximity Engine.
Proximity Server Response Sent	Responses made by the Proximity Engine.
Proximity Server Faults Sent	Faults sent by the Proximity Engine.
Proximity Server Redirect Faults Sent	Faults sent by the Proximity Engine that were redirected requests.

**Viewing Statistics****Viewing IS-IS Statistics**

To view the IS-IS statistics of the Proximity Engine, follow these steps:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the Service Router. The Devices home page is displayed.
  - Step 3** Choose **Statistics > ISIS**. The IS-IS Statistics are displayed.

[Table 8-35](#) describes each IS-IS statistic.

**Table 8-35 IS-IS Statistics**

Statistic	Description
<b>First Section (LAN-IIH, P2P-IIH, CSNP, and PSNP PDU-type packets)</b>	
Interface	From the <b>Interface</b> drop-down list, choose a specific interface or <b>All</b> .
PDU	Packet data unit (PDU) type.
Received	Packets received by IS-IS.
Sent	Packets sent by IS-IS.
RcvAuthErr	Count of messages that failed authorization.
OtherRcvErr	Count of messages that failed due to other errors.
<b>Second Section (LSU PDU-type packets)</b>	
PDU	Packet data unit (PDU) type.
Received	Packets received by IS-IS.
Flooded	Packets flooded by IS-IS.
RcvAuthErr	Count of messages that failed authorization
OtherRcvErr	Count of messages that failed due to other errors.
ReTransmit	Packets retransmitted by IS-IS.
<b>Third Section</b>	
DIS elections	Designated Intermediate System (DIS)
SPF calculations	Shortest path first (SPF) calculation count by IS-IS.
LSPs sourced	Link state packets (LSPs) sourced out by IS-IS.
LSPs refreshed	LSPs refreshed by IS-IS.
LSPs purged	LSPs purged by IS-IS.

---

## Viewing OSPF Statistics

To view the OSPF statistics of the Proximity Engine, follow these steps:

- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
- Step 2** Click the **Edit** icon next to the Service Router. The Devices home page is displayed.
- Step 3** Choose **Statistics > OSPF**. The OSPF Statistics are displayed.

[Table 8-36](#) describes each OSPF statistic.

**Table 8-36 OSPF Statistics**

Statistic	Description
<b>Router Information Changes</b>	
Router ID changes	Total number of OSPF router IDs changed.
DR elections	Total number of OSPF designated router (DR) elections.
Older LSAs received	Total number of older link state advertisements (LSAs) received.
Neighbor state changes	Total number of neighbor state changes.
Neighbor dead postponed	Total number of times a dead neighbor event was postponed.
Neighbor dead interval expirations	Total number of neighbors that exceeded the router dead interval (RDI) and are now considered down.
Neighbor sequence number mismatches	Total number of neighbor sequence mismatches.
SPF computations	Total number of SPF computations.
<b>LSA Statistics</b>	
LSA Type	LSA types consist of Router, Network, Summary Net, Summary autonomous system border router (ASBR), AS External, Opaque Link, Opaque Area, and Opaque AS.
Generated	Total number of LSA packets generated.
Refreshed	Total number of LSA packets refreshed.
Flushed	Total number of LSA packets that were flushed.
Aged out	Total number of LSA packets that were aged out.

**Viewing Statistics****Table 8-36 OSPF Statistics (continued)**

<b>Statistic</b>	<b>Description</b>
<b>Counters</b>	
LSA deletions	<p>Information displayed about the LSA deletions:</p> <ul style="list-style-type: none"> <li>• Pending—Number of LSA deletions that are pending</li> <li>• HWM—High water mark (hwm) of pending deletions</li> <li>• Deleted—Number of LSAs that have been deleted</li> <li>• Revived—Number of LSAs that have been revived</li> <li>• Runs—Number of times the purge routine has run since the OSPF process was started.</li> </ul>
Hello queue	<p>Information displayed about the packets being processed in the hello queue:</p> <ul style="list-style-type: none"> <li>• Current number in queue/maximum number allowed in queue; for example 0/200</li> <li>• High water mark (hwm) is the maximum number of packets ever stored in the queue</li> <li>• Drops are the number of packets dropped because the queue was full.</li> </ul>
Flood queue	Information about the flood queue.
LSDB additions failed	Total number of link state database (LSDB) additions that failed.
Buffers	Memory buffer size.
in use	Amount of the buffer that is currently being used.
hwm	Amount of the buffer that is reserved for the hwm.
permanent	Amount of the buffer that is permanently reserved.
alloc	Amount of the buffer that is currently allocated.
free	Amount of the buffer that is currently free.

## Viewing SRP Statistics

To view the SRP statistics of the Proximity Engine, follow these steps:

- 
- Step 1** Choose **Devices > Devices**. The Devices Table page is displayed.
  - Step 2** Click the **Edit** icon next to the Service Router. The Devices home page is displayed.
  - Step 3** Choose **Statistics > SRP**. The SRP Statistics are displayed.

[Table 8-37](#) describes the SRP statistics for sent, received, and neighbors.

**Table 8-37 SRP Statistics**

Statistic	Description
Join request	Total number of requests packets sent for joining the DHT network.
Join response	Total number of response packets received for joining the DNT network.
LS exchange request	Total number of leafset exchange request packets sent.
LS exchange response	Total number of leafset exchange response packets received.
Route exchange request	Total number of route exchange request packets sent.
Route exchange response	Total number of route exchange response packets received.
Ping request	Total number of DHT ping request packets sent.
Ping response	Total number of DHT ping response packets received.
Lookup request	Total number of lookup request packets sent.
Lookup response	Total number of lookup response packets received.
Ping traceroute request	Total number of ping traceroute request packets sent.
Ping traceroute response	Total number of ping traceroute request packets received.
Request Retry	Total number of request retry packets.
Pkt at wrong interface	Total number of packets received at wrong interface.
Malform packet	Total number of malform packets received.

# Log Files

Log files can generally be categorized into three main classes:

1. Transaction logs
2. Error and debug logs
3. General system logs and core files

## Transaction Logs

Transaction logs are stored under the /local/local1/logs/ directory. They are disabled by default; to enable transaction logging either enter the **transaction-logs enable** command or check the **Transaction Log Enable** check box on the Transaction Log Settings page. See the “[Configuring Transaction Logs](#)” section on page 4-30 for more information.

Transaction log archiving is configured by using the **transaction-logs archive** command or by entering the settings on the Transaction Log Settings page.

To allow the SR Service Monitor module to collect threshold information enter the **service-router service-monitor transaction-log enable** command or check the **Enable** check box for each setting on the Service Monitor page. See the “[Setting Service Monitor Thresholds](#)” section on page 4-83 for more information. To configure the Service Monitor thresholds, use the Service Monitor page.

For more information about transaction logs, see the “[Transaction Logs](#)” section.

## Error and Debug Logs

Error and debug logs are stored under the /local/local1/errorlog/ directory. By default, all software modules only log error related information. Debug logging levels can be controlled (on a per software module basis) through the **debug** command.

There is a background cron job that periodically (every hour) monitors and trims the overall size of SYSFS (including the errorlog/ directory).

## General System Logs and Core Files

General system logs primarily consist of /local/local1/syslog.txt. In addition, any core files generated are stored to the /local/local1/core\_dir/ directory. The same background cron job used for the error and debug logs also monitors and trims the growth of syslog.txt and core\_dir/ directory. If the overall space usage of SYSFS exceeds 80 percent, this cron job raises an alarm indicating that.

When the overall SYSFS space usage exceeds 90 percent, this cron job starts freeing up space by removing the oldest files first. The algorithm used basically removes files based on their age. Initially, all files that are older than 30 days are removed (from the core\_dir/, errorlog/, and logs/ directories). If this does not free up enough space (that is less than 90 percent of capacity), then all files having an age of 10 days are removed.

# 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 Logs](#)” section on page 4-30.

This section discusses the following topics:

- [Transaction Log Formats for Acquisition and Distribution](#)
- [Transaction Log Formats for Web Engine](#)
- [Transaction Logging and NTLM Authentication](#)
- [Usage Guidelines for Log Files](#)
- [Windows Media Transaction Logging](#)
- [Movie Streamer Transaction Log Fields](#)
- [Flash Media Streaming Transaction Log Fields](#)
- [Service Router Transaction Log Fields](#)
- [Service Monitor Transaction Logs](#)
- [Content Manager Transaction Log Fields](#)
- [Web Engine User Level Session Transaction Logs](#)



**Note**

Each transaction log includes a header line that provides the Cisco VDS-IS software version and 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 Acquisition and Distribution

Acquisition and Distribution logs are logged by the following acquisition and distribution processes:

- Unicast Sender
- Unicast Receiver
- Multicast Sender
- Multicast Receiver
- Metadata Sender
- Metadata Receiver
- Acquirer

Acquisition and Distribution logs are located in the local/local1/logs/acqdist directory.

The Acquisition and Distribution log file format is as follows:

StartTime Duration ProcessName DeliveryServiceID DeliveryServiceName DeviceName  
CDNUrl SourceUrl LastModifiedTime Size Status Action AuthType ProxyUsed BillingCookie

Acquisition and Distribution log format examples looks like this:

```
Fri-Feb-28-07:12:01-2014 0 Acquirer 419 <ds> <SE1>
<10.74.7.19/DASH/Envivio/abr_100/test100-32.m4s>
<http://10.74.7.19/DASH/Envivio/abr_100/test100-32.m4s> Wed-Nov-20-10:15:27-2013 1918298
<Success> <Acquire> <none> <none> <->
Fri-Feb-28-07:13:45-2014 0 MetaSender 419 <ds> <SE2>
<10.74.7.19/DASH/Envivio/abr_100/test100-32.m4s>
<http-10.74.7.19-sPkgAACSG2JJqIutGpFmVg/DASH/Envivio/abr_100/test100-32.m4s> - 1
<Complete> <MetaSend> <-> <-> <->
Fri-Feb-28-07:21:15-2014 149 McastSender 419 <ds> <SE1>
<DASH/Envivio/abr_10/test10-10.m4s>
<http-10.74.7.19-sPkgAACSG2JJqIutGpFmVg/DASH/Envivio/abr_10/test10-10.m4s>
Wed-Nov-20-10:12:52-2013 1918298 <Complete> <McastSend> <-> <-> <->
```

## ■ Transaction Logs

```

Fri-Feb-28-07:13:45-2014 0 MetaReceiver 419 <ds> <SE1>
<10.74.7.19/DASH/Envivio/abr_100/test100-32.m4s>
<http-10.74.7.19-sPkgAAcSG2JJqIutGpFmVg/DASH/Envivio/abr_100/test100-32.m4s>
Wed-Nov-20-10:15:27-2013 1 <Success> <MetaReceive> <-> <-> <->
Table 7-36 describes the fields for the Acquisition and Distribution transaction log.
Fri-Feb-28-07:19:57-2014 70 McastReceiver 419 <ds> <10.75.168.28>
<DASH/Envivio/abr_10/test10-1.m4s>
<http-10.74.7.19-sPkgAAcSG2JJqIutGpFmVg/DASH/Envivio/abr_10/test10-1.m4s>
Wed-Nov-20-10:12:34-2013 1918298 <Complete> <McastReceive> <-> <-> <->

```

[Table 8-38](#) describes the fields for the Acquisition and Distribution transaction log.

**Table 8-38      Acquisition and Distribution Transaction Log Fields**

Field	Description
StartTime	The date and time at which the acquisition and distribution process was started.
Duration	The duration in seconds taken to complete the acquisition and distribution process
ProcessName	Name of the Acquisition and Distribution process. The value is one of the following: <ul style="list-style-type: none"> <li>• Acquirer</li> <li>• MetaSender</li> <li>• MetaReceiver</li> <li>• UcastSender</li> <li>• UcastReceiver</li> <li>• McastSender</li> <li>• McastReceiver</li> </ul>
DeliveryServiceID	The Delivery Service id for which the content is being acquired or distributed
DeliveryServiceName	The Delivery Service name for which the content is being acquired or distributed
DeviceName	The Service Engine name that initiated the acquisition or distribution process. <b>Note</b> For Metadata Sender and Metadata Receiver the name of the forwarded SE is logged
CDNUrl	The URL provided by the end client for the data file
SourceUrl	URL used internally by the acquisition and distribution process to refer to CDN URL
LastModifiedTime	The time at which the data file to be acquired or distributed was last modified
Size	The size of the data file to be downloaded/sent/received in bytes

**Table 8-38 Acquisition and Distribution Transaction Log Fields**

Field	Description
Status	<p>The status of acquisition and distribution process on completion. The value is one of the following:</p> <ul style="list-style-type: none"> <li>• Abort —McastReceive failed to update receive status, failed to receive the file, not in receiving state, or the content which McastSend send is stale</li> <li>• Success</li> <li>• Fail</li> <li>• Complete</li> <li>• Continue —The status will be displayed, if content item in acquisition or distribution process is crawl, and displays the sending action is in process</li> <li>• Partial —The status is displayed if the content in UcastReceive is partially received</li> </ul>
Action	<p>The action performed by Multicast Sender/Receiver, Unicast Sender/Receiver and Acquirer during the acquisition/distribution process. The value is one of the following:</p> <ul style="list-style-type: none"> <li>• Acquire</li> <li>• MetaUpdate</li> <li>• Update</li> <li>• Delete</li> <li>• ChannelAdd</li> <li>• ChannelDelete</li> <li>• UcastSend</li> <li>• MetaSend</li> <li>• UcastReceive</li> <li>• MetaReceive</li> <li>• Reschedule —If the UcastReceive is not successful, it will start the reschedule action</li> </ul>
AuthType	<p>It is populated as none by Acquirer and “.” by other processes</p> <p><b>Note</b> This field is just a placeholder and is not used in the 3.2.2 release.</p>

**Table 8-38 Acquisition and Distribution Transaction Log Fields**

Field	Description
ProxyUsed	<p>It is populated as none by Acquirer and “-” by other processes</p> <p><b>Note</b> This field is just a placeholder and is not used in the 3.2.2 release.</p>
BillingCookie	<p>Billing Cookie field used for customer billing transactions in a given streamer configured in the Device Activation page of a device. When not configured “-” is displayed</p> <p><b>Note</b> This field is included starting from release 3.2.2</p>

## Transaction Log Formats for Web Engine

The transaction logs for Web Engine consist of the following:

- [Client Transaction Logs](#)
- [Ingest Transaction Logs](#)

### Client Transaction Logs

The section discusses the following different logging formats for Web Engine:

- [Extended Squid](#)
- [Apache](#)
- [Custom Format](#)



**Note** Changing the time zone on an SE does not affect the log entry nor the log filename. Both the log entries and the log filename always use UTC.



**Note** The timestamp for Web Engine transaction log entry has no space between the date and the time. An example follows:

```
[19/Oct/2010:11:20:09.133-0705] 4821 172.22.71.155 TCP_MISS/404 235 GET
http://172.22.71.155/hello application/octet-stream
```

### Extended Squid

The Extended Squid format logs the same fields logged by the Squid-1.1 access log file format. The Extended Squid transaction logs are located in the logs/webengine\_extsquid/ directory.

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 BillingCookie

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 12334556raaa-USA-NJ
```

**Table 8-39** describes the fields for the Extended-Squid transaction log.

**Table 8-39 Extended-Squid Transaction Log Fields**

Field	Description
Current-Time	Time (milliseconds), in common log time format, the request was received.
Time-to-Serve	Time, in microseconds, taken to complete the request.  This field could be zero if the transaction complete time is greater than the transaction start time, which could occur if NTP is not synchronized.
Client-IP	IP address of the requesting client.
Request-Desc/Status-Returned	Combination of Squid result codes and the response code returned to the client.  The Request-Desc/Status-Returned field includes the error status code for both TCP_MISS and TCP_HIT. A TCP_HIT with an error status code means the HTTP response was served from cache. The meaning of a TCP_MISS with an error status code has not changed.  For more information on troubleshooting a TCP_MISS/504 status code, see the “ <a href="#">Troubleshooting Web Engine Cache Status Codes</a> ” section on page <a href="#">A-7</a> .
Bytes-Xferred	Bytes sent to the client, including the headers.
Method	Request method.
URL	Requested URL, including the query string.
MIME-Type	MIME type.
BillingCookie	Billing Cookie field used for customer billing transactions in a given streamer configured in the Device Activation page of a device. When not configured “-” is displayed
<b>Note</b> This field is included starting from release 3.2.2	

**Table 8-40** describes the Squid codes currently supported. The TCP\_ codes refer to the cache status of the object when the request was handled by the Web Engine. In addition to the cache statistics listed in **Table 8-40**, the client or server error statistics could get incremented as well depending on the response code.

**Table 8-40 Squid Code Request Descriptions**

<b>Squid Result Code</b>	<b>Description</b>	<b>Valid Response (Status) Code</b>	<b>Mapping to Cache Statistics</b>
TCP_MISS	Requested object was not in cache.	0–5xx	Cache miss Cache bypass Partial hit
TCP_MEM_HIT	Valid copy of the requested object was in memory.	Currently supports only 2xx response code	Cache hit and memory hit <b>(show statistics web-engine detail)</b>
TCP_HIT	Valid copy of the requested object was in cache.	0, 2xx, 3xx, 406, 412, 416, 500	Cache hit
TCP_REFRESH_MISS	Requested object was cached but is stale. The query returned the new content.	0–5xx	Cache miss
TCP_REFRESH_HIT	Requested object was cached, but expired. The query for the object resulted in a “304 not modified” message.	0, 2xx, 406, 412, 416, 500	Cache hit
TCP_IMS_HIT	Client issued an IMS request for an object, which was in cache and was not stale.	0, 2xx, 3xx, 500	Cache hit
TCP_DENIED	Access was denied for this request.	403	—
NONE NONE_ABORTED	See <a href="#">Request Description—None and None_Aborted</a> , for the description.	000	—

**Request Description—None and None\_Aborted**

Normally, when a transaction completes, if the cache status is unknown (before the content lookup completes, the cache status is unknown), and the request was not denied by the Authorization Server, the request description that is written to the transaction log is “NONE.”

If a transaction completes because the client aborted the connection, “\_ABORTED” is appended to “NONE.”

If a transaction completes because of an internal Web Engine failure, and there are no more transactions waiting for the process within the session, then the transaction was not aborted; therefore, the “\_ABORTED” is not appended to “NONE.”

Under the conditions described above, because this occurs before the Origin Server is contacted and there is no Authorization Server failure or redirect, the response status code that is written to the transaction log is 000.

## 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. The Apache-style transaction log files are located in the /webengine\_apache/ directory.

The Apache-style log file format is as follows:

client-IP-address URI bytes-sent object-size bytes-received method status time-received time-to-serve  
BillingCookie

An Apache-style log file format example looks like this:

```
171.71.50.197 http://spcdn-se612-5.sanity.spcdn.net/gmedia-0.4gb.wmv 363704065 137
363710748 GET 200 [06/Nov/2007:00:25:32 +0530] 325033158 12334556raaa-USA-NJ
```

[Table 8-41](#) describes the fields for the Apache-style transaction log.

**Table 8-41      Apache-Style Transaction Log Fields**

Field	Description
client-IP-address	IP address of the requesting client
URI	Requested URL, including the query string.
bytes-sent	Bytes sent to client, including the headers.
object-size	Bytes sent to client, excluding the HTTP headers.
bytes-received	Bytes received from client.
method	Request method.
status	HTTP response code for the request.
time-received	Time, in common log time format, the request was received.
time-to-serve	Time, in microseconds, taken to complete the request.
BillingCookie	Billing Cookie field used for customer billing transactions in a given streamer configured in the Device Activation page of a device. When not configured “-” is displayed
<b>Note</b> This field is included starting from release 3.2.2	

## 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 8-42](#) 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 custom transaction logs are located in the /webengine\_clf/ directory.

**■ Transaction Logs**

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
```

Apache and Squid can be represented by the following custom log format patterns:

Apache-style logging with custom patterns: **%a %U %O %b %I %m %>s %t %D**

Squid-style logging with custom patterns:- **%Z %D %a %R/%>s %O %m %U %M**

**Table 8-42 Custom 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.
%B	Bit rate
%c	Time, in common log time format, that the log entry was generated.
%C	Records AuthLOOKupTime   CALLOOKupTime   CacheRouterTime   OSDownloadTime in microseconds granularity.  CacheRouterTime displays only on revalidation scenario. In normal cache-miss use case, the CALLOOKupTime includes the time taken by cache route lookup as well.
%D	Time consumed to serve the request in microseconds
%E	Encryption type (none, AES256CTR, AES256CBC) for session tracking.
%g	Storage URL when URL Resolve rule action is configured in Service Rule file.
%G	Source URL when URL Resolve rule action is configured in Service Rule file.
%h	Remote host (IP address of the requesting client is logged).
%H	Request protocol.
%i	Session ID for session tracking.
%I	Bytes received from the client.
%k	Method of session tracking (cookie, URL query)
%m	Request method.
%f	Billing Cookie used in customer billing transactions
%M	MIME type of the requested asset.
%o	Custom parameter retrieved from HTTP request URL or Session Cookie using the Service Rule:  SessionCustomParameter#integer (RegEx)
%O	Bytes sent to client, including the headers.

**Table 8-42 Custom Log Format String Values (continued)**

Format Token	Value
%p	Client that set up the transport session for the request. The value is one of the following: <ul style="list-style-type: none"> <li>• Local—Request is from this SE.</li> <li>• Internal—Request is from other SE</li> <li>• External—Request is from end user</li> </ul>
%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. The space in the first line of the request is replaced with a vertical bar ( ) delimiter (for example, Get /index.html HTTP/1.1)
%R	Request description (Squid description codes).
%s	Reserved for future use.
%>s	Status. The translog code always returns the HTTP response code for the request.
%S	Session status for session tracking.
%t	Time in common log time format (or standard English format).
%P	Profile string retrieved from URL
%T	Time consumed to serve the request in seconds (a floating point number with 3 decimal places).
%u	URL path requested, including query strings.
%U	URL path requested, not including query strings.
%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.
%y	Session protocol for session tracking.
%X	Connection status when the response is completed. The %X field has the following possible values: <ul style="list-style-type: none"> <li>• X—Connection aborted before the response completed.</li> <li>• +—Connection may be kept alive after the response is sent.</li> <li>• -—Connection is closed after the response is sent.</li> </ul>
%Z	Print the request received time stamp in milliseconds; otherwise, the request received time stamp is in seconds.
%{Header-Field}i	Any request header. Replace the <i>Header-Field</i> with the actual header field you want to log; for example, %{Cache-Control}i. <b>Note</b> All client request headers are only logged on the edge SE.

### Content Flow Trace

Content Flow Trace is used to track the flow of HTTP messages through the VDS-IS and the HTTP response from the Origin Server.

To accomplish this, custom HTTP headers are used for both the requests and the responses. Every tier adds information to the HTTP headers before sending it to the next SE. The custom headers added by the SEs are stripped by the Content Acquirer before the request is sent to the Origin Server. Similarly, the custom headers are stripped from the response before sending it to the client, unless the **Enable Filter Trace Flow to Client** option is enabled.



- Note** The Content Flow Trace is used for debugging potential issues in the VDS-IS and should not be used during high traffic loads.

Content Flow Trace tracks latency in Authorization lookup, CAL lookup, content route lookup, and Origin Server latency. It also keeps track of cache status and response codes.

Custom log format needs to be used to track the request and response headers. The custom log format string to add to the request and response information is the following:

```
transaction-logs format custom "%{CDS-CLIENT-INFO}i %{CDS-RESPONSE-INFO}o"
```

Both the client information and the response information are printed on the same line. They are discussed separately here for clarification.

- Request Header Format

The CDS-CLIENT-INFO is captured on the edge SE and forwarded to all other SEs. The following fields are included in the request header:

- Client\_ip:Client\_port#
- Date\_Time#
- User\_Agent#

Following are examples of the CDS-CLIENT-INFO request headers:

```
192.0.2.95:17836#[03/Jun/2011:11:48:36.871+0000]#Wget/1.10.2#
192.0.2.95:21164#[03/Jun/2011:11:52:29.012+0000]#Wget/1.10.2#
192.0.2.95:28789#[03/Jun/2011:11:59:00.901+0000]#Wget/1.10.2#
```

- Response Header Format

The CDS-RESPONSE-INFO is added on every SE. If the request is sent to the Origin Server, the Origin Server IP address and Origin Server response code are added. The following fields are included in the response header:

- <Hostname>#
- <ResponseCode>#
- <Cache\_Status>#
- AT:<AuthLookupTime>#
- CLT:<CalLookupTime>#
- CRT:<ContentRouteTime>#
- OsLatency:<OSLatency>#

Following are examples of the CDS-RESPONSE-INFO response headers:

- Cache-miss on two tiers. The first line is the Origin Server information, the second line is the Content Acquirer information, and the third line is the edge SE information.

```
192.168.1.12#200|
SE1-2#200#Cache_Miss#AT:855#CLT:453#CRT:0#OSLatency:2104|||
SE2-3#200#Cache_Miss#AT:906#CLT:464#CRT:0#OSLatency:14486|
```

- Cache hit

```
SE1-3#200#Cache_Hit#AT:987#CLT:901#CRT:0#OSLatency:0|
```

- Cache hit with revalidation. The first line is the Origin Server information, the second line is the Content Acquirer information, and the third line is the edge SE information.

```
192.168.1.12#304|
SE1-2#304#Cache_Status_Unknown#AT:243#CLT:673#CRT:0#OSLatency:0|||
SE2-3#200#Cache_Hit#AT:278#CLT:651#CRT:0#OSLatency:2198|
```

## Ingest Transaction Logs

Ingest transaction logs are used to log details of every upstream request sent by the Web Engine to the upstream SEs and origin servers. Ingest transaction logs only stores request details of cache-miss content and cache-hit content with a revalidation request; details of prefetched content are not stored in the ingest transaction logs.

To enable the Web Engine ingest transaction logs, enter the **web-engine http-ingest-logging enable** command.

The Web Engine ingest transaction logs are located in the /local/local1/logs/webengine\_ingestlog\_clf directory.

The ingest log file format is as follows:

```
Time URL FailOverSrvList ServerIP BytesRead BytesToRead AssetSize %DownloadComplete
DownloadTime(Seconds) ReadCallBack Status-Returned MIME-Type Revalidation-Request
CDSDomain ConnectionInfo(LocalPort|ConnectTime|Retry|Reuse) IngestStatus BillingCookie
```

```
Time URL FailOverSrvList ServerIP BytesRead BytesToRead AssetSize %DownloadComplete
Status-Returned MIME-Type Revalidation-Request BillingCookie
```

```
Time URL FailOverSrvList ServerIP BytesRead BytesToRead AssetSize %DownloadComplete
DownloadTime(Seconds) ReadCallBack Status-Returned MIME-Type Revalidation-Request
CDSDomain ConnectionInfo(LocalPort|Protocol|ConnectTime|Retry|Reuse) IngestStatus
RedirectedUrl FailoverAction BillingCookie
```




---

**Note** Billing Cookie field is introduced in Ingest Transaction Logs starting from release 3.2.2

---

An ingest log file example for a cache-miss looks like this:

```
[11/Feb/2011:17:55:51+0000] http://4.0.1.6/sam.html 4.0.1.6/ 4.0.1.6 45 45 45 100 200
text/html; charset=utf-8 No 12334556raaa-USA-NJ
```

An ingest log file example for a cache-hit with a revalidation request looks like this:

```
[11/Feb/2011:17:59:15+0000] http://4.0.1.6/sam.html 4.0.1.6/ 4.0.1.6 0 0 0 0 0 304 -
Yes[If_None_Match: "1d58ac1-2d-230b4c40"]12334556raaa-USA-NJ
```

An ingest log file example if one Origin Server fails looks like this:

**Transaction Logs**

```
[20/Feb/2013:13:03:28.-238+0000] -- 0 0 0 0 -1 0 0 - No - - - FAILOVER_TO[3.4.5.6]
12334556raaa-USA-NJ
```

An ingest log file example if all Origin Servers fails looks like this:

```
[20/Feb/2013:13:03:28.-238+0000] -- 0 0 0 0 -1 0 0 - No - - - NOTIFY_ALL_OS_FAIL
12334556raaa-USA-NJ
```

**Table 8-43** describes the fields for the ingest transaction log.

**Table 8-43 Ingest Transaction Log Fields**

Field	Description
Time	Time the request was sent by the Web Engine to the upstream SE or origin server.  <b>Note</b> The time value for each piece of log is not expected to be strictly incremental
URL	Requested URL, including the query string, sent by the Web Engine.
FailOverSvrList	Hierarchical route look-up information to the upstream SE or origin server. When a cache route look-up is performed for the request, the list of upstream SEs and origin server contacted to fetch the content is included in the log entry.
ServerIP	IP address of the SE or origin server from which the content is downloaded. This is obtained from the FailOverSvrList.
BytesRead	Number of bytes downloaded from the upstream SE or origin server.
BytesToRead	Total number of bytes to be downloaded from the upstream SE or origin server.
AssetSize	Size of the asset (in bytes) requested.
%DownloadComplete	Percentage of asset that has been downloaded to the requesting SE.
DownloadTime(Seconds)	Time, in seconds, to download the incoming stream.
ReadCallBack	Number of read callbacks received to read the response body.
Status-Returned	HTTP status code returned from the upstream SE or origin server.
MIME-Type	MIME type (spaces removed).
Revalidation-Request	Either “Yes” if the request is a revalidation request for a cache hit, or “No” if the request is a cache-miss. If “Yes,” the Header-Name:HeaderValue follows. The “If-None-Match” or “If-Not-Modified” headers and their values are included in the log entry. Spaces are removed.  If the Revalidation header is an etag, the space between the header and colon (If-none-match: "etag ") is removed. If the revalidation header is a date header, the space is replaced by an underscore (_) for readability.
CDSDomain	Internal header added by Web Engine when contacting another SE in the VDS-IS hierarchy. The header value represents the request domain of the end client request.

**Table 8-43      Ingest Transaction Log Fields (continued)**

Field	Description
ConnectionInfo(LocalPort ConnectTime Retry Reuse)	Connection information. This field has the following values: <ul style="list-style-type: none"> <li>• LocalPort—Local port used by the SE to talk to upstream</li> <li>• ConnectTime—Time at which the connection was established</li> <li>• Retry—Number of retries on the connection</li> <li>• Reuse—Number of times the same connection was reused</li> </ul>
IngestStatus	Displays the ingest status. This field has the following value: <ul style="list-style-type: none"> <li>• CONNECT_TIMEOUT</li> <li>• CONNECT_CB SOCK_ERR</li> <li>• CONNECT SOCK_ERR</li> <li>• CONNECT_TO_SELF</li> <li>• WRITE_READY_TIMEOUT</li> <li>• WRITE SOCK_ERR</li> <li>• READ_TIMEOUT_HEADER</li> <li>• READ_TIMEOUT_BODY</li> <li>• READ_RCVD_ON_WRITE</li> <li>• READ SOCK_ERR HEADER</li> <li>• READ SOCK_ERR BODY</li> <li>• HEADER_INVALID_CONT_LEN</li> <li>• HEADER_PARSE_EXCEPTION</li> <li>• HEADER_PARSE_ERR</li> <li>• NO_NEED_TO_GET_BODY</li> <li>• NO_MORE_DATA_TO_READ</li> <li>• HEAD_RESPONSE</li> <li>• SUCCESS_FINISH</li> <li>• INVALID_STATE</li> </ul>
RedirectedUrl	If a 302 response code is received, the RedirectedUrl displays the new URL. If a 200 response code is received, the RedirectedUrl displays no data (-).
FailoverAction	Origin Server failover action. The field has the following values: <ul style="list-style-type: none"> <li>• FAILOVER_TO[FQDN of next OS in OS list]</li> <li>• NOTIFY_ALL_OS_FAIL</li> </ul>
BillingCookie	Billing Cookie field used for customer billing transactions in a given streamer configured in the Device Activation page of a device. When not configured “-” is displayed
	<b>Note</b> This field is included starting from release 3.2.2

## 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](#)
- [Archive Working Log](#)
- [Exporting Log Files](#)



**Note**

---

The time stamp in the filename is always in UTC, but the time stamp for the log entries in the transaction logs are determined by the protocol engine.

---

## Working Logs

Transaction logs are located in the /local/local1/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 /local/local1/logs/export/working.log
- Movie Streamer logs are logged to a working log on the local disk in /local/local1/logs/movie-streamer/working.log
- Flash Media Streaming logs are logged to a working log on the local disk in /local/local1/logs/fms\_access/working.log and /local/local1/logs/fms\_authorization/working.log
- Service Router logs are logged to a working log on the local disk in the /local/local1/logs/service\_router/working.log
- Web Engine client transaction logs are located in the /local/local1/logs/webengine\_apache, the /local/local1/logs/webengine\_clf, and the /local/local1/logs/webengine\_extsquid directories
- Web Engine ingest transaction logs are located in the /local/local1/logs/webengine\_ingestlog\_clf directory
- Service Router transaction logs are located in the /local/local1/logs/service\_router directory
- Service Monitor transaction logs are located in the /local/local1/logs/service\_monitor directory
- Content Manager transaction logs are located in the /local/local1/logs/content\_mgr directory
- Per Session logs are located in the /local/local1/logs/webengine\_abr directory

**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 /local/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 created. The time stamp in the filename is always in UTC, but the time stamp for the log entries in the transaction logs are determined by the protocol engine. 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

*<type>\_<ipaddr>\_yyymmdd\_hhmmss\_<file\_generation\_number>* format, where:

- *<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.
- *yyymmdd\_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.

### 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:

**Transaction Logs**

- 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 zip 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 Logs](#)” section on page 4-30 for SEs, and the “[Configuring Transaction Logs for the Service Router](#)” section on page 4-129 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 export is retried at 10-minute intervals or sooner if the configured export interval is sooner. If the error is a result of a misconfiguration, 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 transaction logs for Windows Media Streaming consist of the following:

- [Windows Media Client Transaction Logs](#)
- [Windows Media Ingest Transaction Log](#)

### Windows Media Client Transaction Logs

The following logging 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 /local/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. The upstream SE can generate the transaction log based on the client information sent at the beginning of the session and information gathered by the SE. In this way, a Windows Media Streaming transaction log always exists for every client session.



#### 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.

### 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.

**Transaction Logs**

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 8-44](#) describes the log formats accepted by Windows Media Services Version 9.0.

**Table 8-44 Windows Media Services Version 9.0 Log Formats**

<b>Protocol</b>	<b>Player and Distributor</b>	<b>Log Type</b>
HTTP/1.0	Windows Media Player earlier than Version 9.0 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 Distribution server is running Windows Media Services Version 9.0 SE (caching and proxy server) is running Windows Media Services Version 9.0	XML structure log
RTSP	Windows Media Player Version 9.0 Distribution server is running Windows Media Services Version 9.0 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 nor the log filename. Both the log entries and the log filename always use UTC.

Table 8-45 describes the fields for the Windows Media Streaming transaction log.

**Table 8-45 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 Multicast
date	Date, in international date format, when a client is connected.	2001-04-19	Unicast 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 Multicast
c-dns	This field is always blank.	—	Unicast Multicast
cs-uri-stem	The path (requested URL without the schema, host, port number, and question mark) to the content that was requested. See cs-uri for the full URL.  <b>Note</b> This represents a change from Windows Media Services version 4.1, in which this field contained the full URL.	/test/sample.wmv or /broadcast	Unicast 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 Multicast
x-duration	The x-duration field has the value based on the following: <ul style="list-style-type: none"><li>• If the client does not report a value, indicated by a hyphen (-), the server value is used.</li><li>• If the value is reported as zero, then the server duration value is used.</li><li>• If the server compares the x-duration reported by the client with the filelength and the difference is more than two minutes, then the server's duration value is used.</li></ul>	31	Unicast Multicast
c-rate	The rate at which data is sent from the server to the client. The c-rate field has the following possible values: <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> If you are using Fast Streaming, these values could be considerably higher or lower depending on the content and the available bandwidth.	1	Unicast Multicast

**■ Transaction Logs****Table 8-45 Windows Media Streaming Transaction Log Fields (continued)**

<b>Field</b>	<b>Description</b>	<b>Sample Value</b>	<b>Client Data Reported</b>
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 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-xxxxxxxxxx}, where x is the session ID of the client. For distribution server log entries, this value is always a series of zero's.	{c579d042-cecc-11d1-bb31-00a0c9603954}	Unicast 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 Multicast
c-playerlanguage	Language and country or region code of the player.	en-US	Unicast 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. The user-agent value is enclosed in double quotes ("").	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 vb.exe mplayer2.exe WMServer.exe	Unicast Multicast
c-hostexever	Host program (.exe) version number.	4.70.1215	Unicast Multicast

**Table 8-45 Windows Media Streaming Transaction Log Fields (continued)**

<b>Field</b>	<b>Description</b>	<b>Sample Value</b>	<b>Client Data Reported</b>
c-os	Client operating system.	Windows_NT	Unicast Multicast
c-osversion	Version number of the client operating system.	4.0.0.1381	Unicast Multicast
c-cpu	Client CPU type.	Pentium	Unicast 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 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 Multicast
transport	Transport protocol used to stream the content. Multicast content is always streamed using UDP.	UDP TCP	Unicast 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 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 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 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.  This field contains a hyphen (-) in propagated cache or proxy logs and in multicast log files.	30000	Unicast

**■ Transaction Logs****Table 8-45 Windows Media Streaming Transaction Log Fields (continued)**

<b>Field</b>	<b>Description</b>	<b>Sample Value</b>	<b>Client Data Reported</b>
c-bytes	<p>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.</p> <p><b>Note</b> It may seem that if the sc-bytes and the c-bytes field are not identical that it indicates packet loss. However, if the c-status field contains “408,” the c-bytes and sc-bytes are not identical, which does not indicate packet loss.</p>	28583	Unicast Multicast
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 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 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 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 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 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 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 Multicast

**Table 8-45 Windows Media Streaming Transaction Log Fields (continued)**

<b>Field</b>	<b>Description</b>	<b>Sample Value</b>	<b>Client Data Reported</b>
c-buffercount	Number of times the client buffered while playing the stream.	4	Unicast 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 Multicast
c-quality	The lowest amount of stream quality reported by the player during the playback of the stream.	96	Unicast Multicast
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 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 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
	<b>Note</b> Windows Media Services Version 9.0 (standard and extended) field.		
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
	<b>Note</b> Windows Media Services Version 9.0 (standard and extended) field.		
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/WMRoot\Encoder_ad.wmv or http://www.example.microsoft.com/speech.wma	Unicast
	<b>Note</b> Windows Media Services Version 9.0 (standard and extended) field.		

**Table 8-45 Windows Media Streaming Transaction Log Fields (continued)**

Field	Description	Sample Value	Client Data Reported
cs-uri	<p>In general, the cs-uri has the SE name in the URL, but in the case of IPFWD or DNS-based routing, the redirection URL without the SE name is included. Basically, the cs-uri has the full URL requested by the client.</p> <p>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.</p> <p><b>Note</b> Windows Media Services Version 9.0 (standard and extended) field.</p>	mms://microsoft.com/mycontent.wmv asfm://206.73.118.254:26502  For Windows Media Player 9 Series clients: asfm://multicast IP address:port/Server IP address	Unicast Multicast
cs-media-name	<p>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.</p> <p>Alternatively, this entry can be specified in the announcement file to classify logs according to user or content.</p> <p><b>Note</b> Windows Media Services Version 9.0 (standard and extended) field.</p>	/ads/MyAd2.asf	Unicast
c-max-bandwidth	<p>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:</p> <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> <p><b>Note</b> Windows Media Services Version 9.0 (standard and extended) field.</p>	384000	Unicast Multicast
cs-media-role	<p>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.</p> <p><b>Note</b> Windows Media Services Version 9.0 (standard and extended) field.</p>	Ad	Unicast

**Table 8-45 Windows Media Streaming Transaction Log Fields (continued)**

<b>Field</b>	<b>Description</b>	<b>Sample Value</b>	<b>Client Data Reported</b>
s-proxied	<p>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.</p> <p><b>Note</b> Windows Media Services Version 9.0 (standard and extended) field.</p>	1	Unicast
SE-action	<p>Indicates the service type from the SE perspective. The value is one of the following:</p> <ul style="list-style-type: none"> <li>• CACHE_MISS—Request is served by SE as cache-miss or partial cache-hit</li> <li>• CACHE_HIT—Request is served by SE as cache-hit, which means all of bytes are served from SE local cache.</li> <li>• VOD—Request is served by SE as prefetched-hit.</li> <li>• live_create—Request is served by SE as live content</li> </ul> <p><b>Note</b> Extended Windows Media Services (Version 4.1 and Version 9.0) field.</p>	VOD	Unicast
SE-bytes	<p>Bytes sent from the SE local cache. This value is “–” if the SE-action is CACHE_MISS or live_create.</p> <p><b>Note</b> Extended Windows Media Services (Version 4.1 and Version 9.0) field.</p>	9600	Unicast
Username	<p>The user name the client provided during authentication from SE side of view. This value should be a duplicate of cs-username, the only difference is cs-username is provided by the client, and this value is determined by the SE during the SE authentication and authorization of the client.</p> <p><b>Note</b> Extended Windows Media Services (Version 4.1 and Version 9.0) field.</p>	JSmith	Unicast
entry-gen-time	<p>Time, in common log time format, that the log entry was generated.</p> <p><b>Note</b> Extended Windows Media Services Version 9.0 field.</p>	[21/Mar/2012:04:05:45.337+0000]	Unicast
mime-type	<p>MIME type.</p> <p><b>Note</b> Extended Windows Media Services Version 9.0 field.</p>	application/octet-stream	Unicast
client-type	<p>Client that set up the transport session for the request. The value is one of the following:</p> <ul style="list-style-type: none"> <li>• Local—Request is from this SE.</li> <li>• Internal—Request is from other SE</li> <li>• External—Request is from end user</li> </ul> <p><b>Note</b> Extended Windows Media Services Version 9.0 field.</p>	External	Unicast

## Windows Media Ingest Transaction Log

The Windows Media Ingest transaction log is a new log file that is used to record the details about dynamically ingested content. The Windows Media Ingest transaction log can be used by the CDNM to generate statistics on gigabytes used for cache-fill of dynamically ingested content by the Windows Media Streaming engine.

The Windows Media Ingest transaction log filename has the following format:

wmt\_ ingestlog\_clf\_<ipaddr>\_yyyymmdd\_hhmmss\_>, where

- <ipaddr> represents the IP address of the SR
- yyyymmdd\_hhmmss represents the date and time when the log was created

The Windows Media Ingest transaction log file is located in the /local/local1/logs/wmt\_ ingest\_clf/ directory on the SE.

[Table 8-43](#) describes the fields for the Windows Media Ingest transaction log.

**Table 46      Ingest Transaction Log Fields**

Field	Description
Time	Time the request was sent by Windows Media Streaming to the upstream SE or origin server.
URL	Requested URL, including the query string, sent by Windows Media Streaming.
FailOverSrvList	Hierarchical route look-up information to the upstream SE or origin server. When a cache route look-up is performed for the request, the list of upstream SEs and origin server contacted to fetch the content is included in the log entry.
ServerIP	IP address of the SE or origin server from which the content is downloaded. This is obtained from the FailOverSrvList.
BytesRead	Number of bytes downloaded from the upstream SE or origin server.
AssetSize	Size of the asset (in bytes) requested.
DownloadTime(Seconds)	Time, in seconds, to download the incoming stream.
Status-Returned	Status code returned from the upstream SE or origin server.
ConnectionInfo(LocalPort ConnectTime Retry Reuse)	Connection information. This field has the following values: <ul style="list-style-type: none"> <li>• LocalPort—Local port used by the SE to talk to upstream</li> <li>• ConnectTime—Time at which the connection was established</li> <li>• Retry—Number of retries on the connection</li> </ul>
IngestStatus	Displays the ingest status. This field has the following value: <ul style="list-style-type: none"> <li>• FAIL</li> <li>• SUCCESS</li> </ul>

## Movie Streamer Transaction Log Fields

**Note**

Changing the time zone on an SE does not affect the log entry nor the log filename. Both the log entries and the log filename always use UTC.

[Table 8-47](#) describes the fields for the Movie Streamer transaction log.

**Table 8-47      Movie Streamer Transaction Log Fields**

Field	Description
c-ip	Client IP address.
date	Current log entry creation date.
time	Current log entry creation time.
c-dns	Always returns a dash (-).
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.

**Table 8-47 Movie Streamer Transaction Log Fields (continued)**

Field	Description
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.
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. [Table 8-48](#) describes the fields for the Flash Media Streaming access log.



**Note** The data in a field can contain a space. The only supported delimiter is a Tab. 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. 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 8-48](#):

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 nor the log filename. Both the log entries and the log filename always use UTC.

**Table 8-48 Flash Media Streaming Access Log Fields**

Field	Description
x-event	Type of event. See <a href="#">Table 8-50</a> for a list of the event types.
x-category	Event category. See <a href="#">Table 8-50</a> for a list of the event categories.
date	Date of the event.
time	Time the event occurred.
tz	Time zone information.
x-ctx	Event-dependent context information.
s-ip	IP address or addresses of the server.

**Table 8-48 Flash Media Streaming Access Log Fields (continued)**

Field	Description
x-pid	Server process ID.
x-cpu-load	CPU load.
x-mem-load	Memory usage (as reported by the getServerStats() method).
x-adaptor	Adaptor name.
x-vhost	Virtual host name.
x-app	Application names.
x-appinst	Application instance names.
x-duration	Duration of a stream or session event.
x-status	The status code. The status code is a ten-character string that represents the severity, category, and message ID.  <b>Note</b> For information on the event status codes for the access log, see the “Event Status Codes in Flash Media Streaming Access Logs” section on page 8-86.  The first three characters represent severity and have the following values: <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>• (u)—Unknown</li> </ul> The next three characters represent the category and have the following values: <ul style="list-style-type: none"> <li>• 257—TCService</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—TCAplication</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> 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> .
c-ip	Client IP address.
c-proto	Connection protocol (RTMP or RTMPT).
c-proto-ver	Connection protocol version.
s-uri	URI of the Flash Media Server application.
cs-uri-stem	The stem portion of the s-uri field.
cs-uri-query	The query portion of the s-uri field.
c-referrer	URI of the referrer.

**Table 8-48 Flash Media Streaming Access Log Fields (continued)**

<b>Field</b>	<b>Description</b>
c-user-agent	User agent. The user-agent value is enclosed in double quotes ("").
c-client-id	Client ID.
cs-bytes	This field shows the number of bytes transferred from the client to the server. 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.
sc-bytes	This field shows the number of bytes transferred from the server to the client. 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
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>
x-sname	Stream name.
x-sname-query	Query portion of the stream URI specified in play or publish.
x-suri-query	Same as x-sname-query.
x-suri-stem	This is a composite field made up of cs-uri-stem + x-sname + x-file-ext.
x-suri	This is a composite field made up of cs-uri-stem + x-sname + x-file-ext + x-sname-query.
x-file-name	Full path of the file representing the x-sname stream.
x-file-ext	Stream type (FLV or MP3).
x-file-size	Stream size in bytes.
x-file-length	Stream length in seconds.
x-spos	Stream position.
c-spos	The client stream position when a “client-pause” or “client-seek” event is logged.
cs-stream-bytes	This field shows the number of bytes transferred from the client to the server per stream. 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.

**Table 8-48 Flash Media Streaming Access Log Fields (continued)**

Field	Description
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>
x-service-name	Name of the service providing the connection (only applicable to certain connection types).
x-sc-qos-bytes	Number of bytes sent to the client for quality of service.
x-comment	Comments.
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.
x-sid	The ID of a stream. This ID is unique for the client session but not across sessions.
x-trans-sname	The name of the stream that the server transitions from (the original stream).
x-trans-sname-query	The query stream portion of the stream name for the stream that the server transitions from.
x-trans-file-ext	The file extension portion of the stream name for the stream that the server transitions from.
x-trans-mode	The transition mode sent by the client in the NetStream.play2() call.
x-soffset	When a stream is reconnected, the offset value indicates where to resume streaming.
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.
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.
x-plugin	Name of the plug-in. This field is only available in authorization (auth-) events.
x-page-url	The URL of the web page in which the client SWF file is embedded.
x-smax-rec-size	The maximum file size of a recorded stream.
x-smax-rec-duration	The maximum duration of a recorded stream.
x-forwarded-for	A string inserted by an HTTP proxy that usually contains the IP address of the originating client. This string can contain several IP address or other values. Flash Media Server copies the string and reports it unchanged.

## Event Status Codes in Flash Media Streaming Access Logs

The event status codes are based on HTTP response codes. [Table 8-49](#) describes the status codes for the Flash Media Streaming access log.

**Table 8-49 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 8-49 Flash Media Streaming Event Status Codes (continued)**

<b>Field</b>	<b>Symbol</b>	<b>Status Code</b>	<b>Description</b>
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	~fcstreamjshook() clean up.

## Events in Flash Media Streaming Access Logs

[Table 8-50](#) describes the event types in the Flash Media Streaming access log and the associated category for each event.

**Table 8-50 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 8-50 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 nor the log filename. Both the log entries and the log filename always use UTC.

The Service Router transaction logs are located in the /local/local1/logs/service\_router directory. Table 8-51 describes the fields for the Service Router transaction log.

**Table 8-51 Service Router Transaction Log Fields**

Field	Description
c-ip	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. The user-agent value is enclosed in double quotes ("").
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	URL requested by the client.

**Table 8-51 Service Router Transaction Log Fields (continued)**

Field	Description
protocol	Protocol used to access the content.
server-picked	Service Engine selected by the Service Router.
routed-path	Path of the redirected URL that is used for last-resort error-domain redirects and last-resort translator API requests.
status	Status code.
routing-method	Routing method chosen. The routing-method field has the following possible values: <ul style="list-style-type: none"> <li>• Last-Resort</li> <li>• Network</li> <li>• Proximity</li> <li>• Zero-Network</li> <li>• Geo-Location</li> </ul>



**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 1-46.

## Service Monitor Transaction Logs

Service Monitor transaction logs provide a tool for analyzing the health history of a device and the protocol engines, to ensure the device is within the configured capacity limits.

The device and service health information are periodically logged on the device in transaction log files. Transaction logs provide a useful mechanism to monitor and debug the system. The transaction log fields include both device and protocol engine information applicable to Service Engines and Service Routers that are useful for capacity monitoring. Additionally, when a device or protocol engine threshold is exceeded, detailed information is sent to a file (threshold\_exceeded.log) to capture the processes that triggered the threshold alarm. To configure threshold settings, see the “[Setting Service Monitor Thresholds](#)” section on page 4-83.

The Service Monitor transaction log filename has the following format:  
service\_monitor\_<ipaddr>\_yyyymmdd\_hhmmss\_<>, where:

- <ipaddr> represents the IP address of the SE, SR, or CDSM.
- yyyymmdd\_hhmmss represents the date and time when the log was created.

For example, service\_monitor\_192.168.1.52\_20110630\_230001\_00336 is the filename for the log file on the device with the IP address of 192.168.1.52 and a time stamp of June 30, 2011 at 3:36 AM.

The Service Monitor transaction log file is located in the /local/local1/logs/service\_monitor directory. An entry to the Service Monitor transaction log is made every two seconds.



**Note** The following rules apply to Service Monitor transaction logs:

- A transaction log value is only logged if the Service Monitor is enabled for that component or protocol engine on the device. For example if CPU monitoring is not enabled, the transaction log value “–” is displayed.
- If Service Monitor is enabled for a protocol engine, but the protocol engine is not enabled, the value is not displayed in the log file.
- If a log field can have more than one value, the values are delimited by the pipe (|) character.
- If a value can have sub-values, the sub-values are delimited by the carrot (^) character.
- Some of the fields display aggregate values. If the statistics are cleared using the clear statistics command, the value after clearing the statistics may be less than the previous values, or may be zero (0).

[Table 8-52](#) describes the fields for the Service Monitor transaction log on an SE.

**Table 8-52 SE Service Monitor Transaction Log Fields**

Field	Sample Output	Description	Corresponding CLI Command
date	2011-06-30	Date of log.	–
time	22:52:02	Time of log.	–
cpu_avg	21	Moving average value in percentage of CPU usage.	show service-router service-monitor Device status—CPU—Average load
mem_avg	44	Moving average value in percentage of memory usage.	show service-router service-monitor Device status—Mem—Average used memory
kernel-mem-avg	11	Moving average value in percentage of kernel memory.	show service-router service-monitor Device status—KMEM—Average kernel memory
disk_avg	2	Moving average value in percentage of disk usage.	show service-router service-monitor Device status—Disk—Average load
disk_fail_count_threshold	Y	Boolean value to indicate if disk fail count threshold has been reached.	show service-router service-monitor Device status—Device Status—Disk—Status
per_disk_load	disk03-01^2 disk04-02^5	Current load per disk, as a percentage. The sample output indicates that disk03—partition01 has a 2 percent load and disk04—partition02 have a 5 percent load.	–
bandwidth_avg	Port_Channel_1^2^4 Port_Channel_2^0^0	Moving average bandwidth used, as a percentage, of bandwidth in and bandwidth out per interface. The sample output indicates that port channel 1 has an average bandwidth of 2 percent for receiving and 4 percent for transmitting, and port channel 2 average bandwidth usage is 0.	<b>show service-router service-monitor</b> Device status—NIC—Average BW In/ Average BW Out

**■ Transaction Logs****Table 8-52 SE Service Monitor Transaction Log Fields (continued)**

<b>Field</b>	<b>Sample Output</b>	<b>Description</b>	<b>Corresponding CLI Command</b>
file-desc-count	1023	Total count of file descriptors open on the device. File descriptors are internal data structures maintained by the Linux kernel for each open file.	<b>show statistics lsof</b>
tcp_server_connections	35	Number of TCP server connections open.	<b>show statistics tcp</b> TCP Statistics—Server connection openings
tcp_client_connections	24	Number of TCP client connections open.	<b>show statistics tcp</b> TCP Statistics—Client connection openings
processes_count	42	Number of processes running on the device.	<b>show processes</b>
dataserver-cpu-percentage	1	Percentage of the CPU used for the dataserver process.	—
movie-streamer-threshold-exceeded	—	Boolean value to indicate if the Movie Streamer threshold has been exceeded.	<b>show service-router service-monitor</b> Services status—MS—Threshold
movie-streamer-augment-threshold-exceeded	—	Boolean value to indicate if Movie Streamer augmentation alarm threshold has been exceeded.	—
movie-streamer-stopped	—	Boolean value to indicate if the Movie Streamer protocol engine has stopped.	<b>show service-router service-monitor</b> Services status—MS—Stopped
movie-streamer-rtsp-sessions-count	—	Total Movie Streamer RTSP session count (aggregate value).	<b>show statistics movie-streamer all</b> Total RTSP sessions
movie-streamer-rtp-sessions-count	—	Total Movie Streamer RTP session count (aggregate value).	<b>show statistics movie-streamer all</b> Total RTP connections
fms_threshold_exceeded	N	Boolean value to indicate if threshold is exceeded.	<b>show service-router service-monitor</b> Services status—FMS—Threshold
fms-augment-threshold-exceeded	N	Boolean value to indicate if Flash Media Streaming augmentation alarm threshold has been exceeded.	—
fms_stopped	N	Boolean value to indicate if Flash Media Streaming has stopped.	<b>show service-router service-monitor</b> Services status—FMS—Stopped
fms_connections_count	2	Total Flash Media Streaming connection count (aggregate value).	<b>show statistics flash-media-streaming</b> Connections—Total
web_engine_threshold_exceeded	Y	Boolean value to indicate if the Web Engine threshold has been exceeded.	<b>show service-router service-monitor</b> Services status—Web—Threshold
web-engine-augment-threshold-exceeded	Y	Boolean value to indicate if Web Engine augmentation alarm threshold has been exceeded.	—
web_engine_stopped	N	Boolean value to indicate if Web Engine has stopped.	<b>show service-router service-monitor</b> Services status—Web—Stopped

**Table 8-52 SE Service Monitor Transaction Log Fields (continued)**

<b>Field</b>	<b>Sample Output</b>	<b>Description</b>	<b>Corresponding CLI Command</b>
web-engine-cpu-percentage	3	Percentage of the CPU used by the Web Engine.	—
web_engine_mem	3500	Memory (in bytes) used by the Web Engine.	<b>show web-engine health</b> Total memory usage
web_engine_get_requests	250	Count of get requests received by the Web Engine (Aggregate value)	<b>show statistics web-engine detail</b> HTTP Request Type Statistics—Get requests
web_engine_sessions	5	Count of HTTP connections.	<b>show statistics web-engine detail</b> Web-Engine Detail Statistics—Total HTTP Connection + Active Session
web_engine_upstream_connections	2	Count of HTTP connections to upstream SE or origin server.	<b>show statistics web-engine detail</b> Web-Engine Detail Statistics—Total HTTP Connection
wmt_threshold_exceeded	N	Boolean value to indicate if Windows Media Streaming threshold has been exceeded.	<b>show service-router service-monitor</b> Services status—WMT—Threshold
wmt-augment-threshold-exceeded	N	Boolean value to indicate if the Windows Media Streaming augmentation alarm threshold has been exceeded.	—
wmt_stopped	Y	Boolean value to indicate if Windows Media Streaming has stopped.	<b>show service-router service-monitor</b> Services status—WMT—Stopped
wmt-ml-cpu-percentage	21	Percentage of the CPU used by the WMT_ML process.	—
wmt-ml-mem	32456	Memory (in bytes) used by WMT_ML process	—
wmt-core-cpu-percentage	21	Percentage of the CPU used by the WMT_Core process.	—
wmt-core-mem	32456	Memory (in bytes) used by the WMT_Core process.	—
wmt-unicast-sessions	22	Number of current concurrent unicast client sessions.	<b>show statistics wmt usage</b> Concurrent Unicast Client Sessions—Current
wmt-remote-sessions	24	Number of current concurrent remote server sessions.	<b>show statistics wmt usage</b> Concurrent Remote Server Sessions
wmt_live_requests	21	Total count of Windows Media Streaming live requests (Aggregate value).	<b>show statistics wmt requests</b> By Type of Content—Live content
wmt_vod_requests	22	Total count of Windows Media Streaming VOD requests (Aggregate value).	<b>show statistics wmt requests</b> By Type of Content—On-Demand Content

■ Transaction Logs
**Table 8-52 SE Service Monitor Transaction Log Fields (continued)**

<b>Field</b>	<b>Sample Output</b>	<b>Description</b>	<b>Corresponding CLI Command</b>
wmt_http_requests	11	Total count of Windows Media Streaming HTTP requests (Aggregate value).	<b>show statistics wmt requests</b> By Transport Protocol—HTTP
wmt_rtsp_requests	8	Total count of Windows Media Streaming RTSP requests (Aggregate value).	<b>show statistics wmt requests</b> By Transport Protocol—RTSPT/RTSPU
rtspg_tps	12	Current RTSP Gateway transactions per second (TPS).	—
uns-cpu-percentage	3	Percentage of CPU used by the Unified Namespace (UNS) process.	—
uns_mem	3500	Memory used by the UNS process.	—

Table 8-53 describes the fields for the Service Monitor transaction log on a SR.

**Table 8-53 SR Service Monitor Transaction Log Fields**

<b>Field</b>	<b>Sample Output</b>	<b>Description</b>	<b>Corresponding CLI Command</b>
date	2011-06-30	Date of log.	—
time	22:52:02	Time of log.	—
cpu_avg	21	Moving average value in percentage of CPU usage.	<b>show service-router service-monitor</b> <b>Device status—CPU—Average load</b>
mem_avg	44	Moving average value in percentage of memory usage.	<b>show service-router service-monitor</b> <b>Device status—Mem—Average used memory</b>
kernel-mem-avg	11	Moving average value in percentage of kernel memory.	<b>show service-router service-monitor</b> Device status—KMEM—Average kernel memory
disk_avg	2	Moving average value in percentage of disk usage.	<b>show service-router service-monitor</b> Device status—Disk—Average load
disk_fail_count_threshold	Y	Boolean value to indicate if disk fail count threshold has been reached.	<b>show service-router service-monitor</b> Device status—Device Status—Disk—Status
file-desc-count	1023	Total count of file descriptors open on the device. File descriptors are internal data structures maintained by the Linux kernel for each open file.	—
tcp_server_connections	35	Number of TCP server connections open.	<b>show statistics tcp</b> TCP Statistics—Server connection openings
tcp_client_connections	24	Number of TCP client connections open.	<b>show statistics tcp</b> TCP Statistics—Client connection openings

**Table 8-53 SR Service Monitor Transaction Log Fields (continued)**

<b>Field</b>	<b>Sample Output</b>	<b>Description</b>	<b>Corresponding CLI Command</b>
processes_count	42	Number of processes running on the device.	<b>show processes</b>
dataserver-cpu-percentage	1	Percentage of the CPU used for the dataserver process.	—
sr-cpu-percentage	12	Cpu percentage used by SR.	—
sr_mem	750000	Memory (in bytes) used by SR.	<b>show processes memory</b> and search for service_router
requests_received	34	Total count of requests received by SR (aggregate value)	<b>show statistics service-router summary</b> Requests Received
http_normal_requests_received	5	Total count of normal HTTP requests received by SR (aggregate value).	<b>show statistics service-router summary</b> HTTP Requests (normal)
http_asx_requests_received	5	Total count of ASX HTTP requests received by SR (aggregate value).	<b>show statistics service-router summary-HTTP Requests (ASX)</b>
rtsp_requests_received	5	Total count of RTSP requests received by SR (aggregate value).	<b>show statistics service-router summary</b> RTSP Requests
rtmp_requests_received	5	Total count of RTMP requests received by SR (aggregate value).	<b>show statistics service-router summary</b> RTMP Requests
dns_requests_received	6	Total count of DNS requests received by SR (aggregate value).	<b>show statistics service-router dns</b> Total DNS queries

## Content Manager Transaction Log Fields

The Content Manager transaction log filename has the following format:

content\_mngr\_<ipaddr>\_yyyymmdd\_hhmmss\_>, where:

- <ipaddr> represents the IP address of the SE, SR, or CDSM.
- yyyymmdd\_hhmmss represents the date and time when the log was created.

The Content Manager transaction log file is located in the /local/local1/logs/content\_mngr directory.

[Table 8-54](#) describes the fields for the Service Monitor transaction log on an SE.

**Table 8-54 Content Manager Transaction Log Fields**

<b>Field</b>	<b>Description</b>
Date	Date of log entry.
Time	Time of log entry.
ContentType	Type of content, which is either cached or prepos-content (prefetched).
Operation	Content Manager operation, which is addition, deletion, update, or eviction.

**Table 8-54 Content Manager Transaction Log Fields (continued)**

Field	Description
Priority	Prefetched content always has a priority of 0, which means ignore. The lower the number, the lower the priority.
CreationDate	Date the content object was created.
CreationTime	Time the content object was created.
FileSize	File size, in bytes, of the content object.
HitCount	Number of times the content object was accessed.
URL	URL of the content object. If Content Manager cannot retrieve the URL by using the FastCAL lookup of the disk path, then the ContentType field has a value of “unknown-content” and the URL field displays “-.”
Path	Disk path of the content object.

## Web Engine User Level Session Transaction Logs

Web Engine User Level Session Transaction Logs consists of two aspects:

1. Adding optional fields that provides information on User Level Session HTTP transactions to the custom format transaction logs for the Web Engine.
2. Enabling the new log file, the Per Session log, which significantly reduces the log message volume by combining per-transaction logs for each session.

### Enabling Per Session Log

To enable Per Session log, the following needs to be configured:

- Each device needs to have transaction logs and per Session logs enabled
- Each Delivery Service must have session tracking enabled
- Service Rule XML file must have a SessionResolveRule configured

#### Enabling Per Session Log on a Device

The transaction logs and Per Session Log must be enabled on each SE participating in session logging.

For more information, see the “Configuring Transaction Logs” section on page 4-30.

#### Enabling Session Tracking for a Delivery Service

To enable session tracking for a Delivery Service, the following must be enabled:

- **Enable Generic Session Tracking**—Enables Generic session tracking at all locations
- **Enable HSS Session Tracking**—Enables HSS session tracking at all locations
- **Enable HLS Session Tracking**—Enables HLS session tracking at all locations

See the “General Settings” section on page 5-21, for more information.

#### Adding a SessionResolveRule to the Service Rule XML File

At least one SessionResolveRule is required to enable the Session log. The Origin server (OFQDN) and Service Routing Domain Name (RFQDN) must be specified as the pattern lists to match for the SessionResolveRule. Following is an example of the SessionResolveRule.

```

<CDSTRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSTRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Demo</CustomerName>
    <ApplyAllTier>yes</ApplyAllTier>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <Domain>msi-cds.com</Domain>
        </PatternListGrp>
        <PatternListGrp id = "grp2">
            <Domain>os-msi-cds.com</Domain>
        </PatternListGrp>    </Rule_Patterns>
    <Rule_Actions>
        <Rule_Allow matchGroup="grp1,grp2" protocol="http"/>
        <Rule_SetAction name="Rule_DSConfig" matchGroup="grp1,grp2" protocol="http">
            <SetParameter name="SessionResolveRule#1" value="m3u8:none"/>
        </Rule_SetAction>
    </Rule_Actions>
</CDSTRules>

```



**Note** In this Service Rule XML file example, the StreamerSecretKey SetParameter for the Rule\_DSConfig Rule\_SetAction is not configured, which results in a warning message. The StreamerSecretKey is used to generate and validate the session cookie MD5 hash. If the StreamerSecretKey parameter is not configured, the default is NULL.

## Web Engine Custom Formats for ABR and Generic Session HTTP Transactions

Each user level streaming session consists of multiple HTTP transactions. Reflected in the transaction logs for Web Engine, there are multiple transaction log entries for one streaming session.

The following custom format tokens have been added to the Web Engine custom format to provide information on User Session HTTP transactions:

- %i—Session ID
- %S—Session status
- %y—Session protocol
- %E—Encryption type (none, AES256CTR, AES256CBC)
- %k—Method of session tracking (cookie, URL query)
- %B—Bitrate
- %P—Profile string retrieved from URL
- %o—Custom parameter retrieved from HTTP request URL or Session Cookie using the Service Rule:  
SessionCustomParameter#integer (RegEx)

Use the **transaction-logs format custom** command to modify the custom log format.

The custom transaction logs are located in the /local/local1/logs/webengine\_clf/ directory.

## Per Session Log

Typically, Session HTTP transaction log volume is very large because of the number of fragments for each session. The Per Session log reduces log message volume by consolidating per-transaction (per fragment) log entries for each session. All Session-related HTTP transactions are logged in the Per HTTP transaction log and session log entries are only generated on session events. The Per Session log is located in the /local/local1/logs/webengine\_abr directory.

### Session Events

HTTP is a stateless protocol. HTTP User Level session does not have a counterpart of states as does the traditional streaming protocol such as RTSP. Session events are defined to help understand when and how session-based transaction log are generated.

[Table 8-55](#) describes the session events for HTTP User level session.

**Table 8-55 Session Events**

Session Event	Description
Session Start	First request for the session is received.
Session Play	First fragment request is received, or first fragment request after a stop event is received.
Bitrate Upshift	Bitrate of requested fragment is faster than the previously requested fragment.
Bitrate Downshift	Bitrate of requested fragment is slower than the previously requested fragment.
Session Stop	Time interval is defined by SessionInactivityTimeout in the rule file. The default value is 10 seconds.
Session Close	There has been no session activity for the duration of the configured session idle time (SessionIdleTimeout parameter is configured in Service Rule XML file).

The following events generate a transaction log entry:

- Session Start
- Session Play
- Bitrate Upshift
- Bitrate Downshift
- Session Stop
- Session Close

The transaction log format for session logging is as follows:

```
client-ip abr-protocol session-id manifest-uri asset-id bytes-sent bytes-recvd status
time-recvd time-to-serve bitrate encryption session-tracking-mode status-code user-agent
entry-gen-time mime-type profile custom-parameter
```

A transaction log file example triggered by Session Start event looks like this:

```
10.140.8.24 hls 6a8-I-617F442F03277469298A3C17657B56C43529
http://hls.abr.com/sample/sample.m3u8 - 0 0 start [25/Sep/2012:11:11:59.326+0000] 0 0 none
cookie 0 "AppleCoreMedia/1.0.0.9B206 (iPad; U; CPU OS 5_1_1 like Mac OS X; zh_cn)"
[25/Sep/2012:11:11:59.350+0000] -- -
```

A transaction log file example triggered by Session Play event looks like this:

```
10.140.8.24 hls 6a8-I-617F442F03277469298A3C17657B56C43529
http://hls.abr.com/sample/sample.m3u8 - 235 436 play [25/Sep/2012:11:11:59.890+0000] 2155
96000 none cookie 200 "AppleCoreMedia/1.0.0.9B206 (iPad; U; CPU OS 5_1_1 like Mac OS X;
zh_cn)" [25/Sep/2012:11:11:59.914+0000] video/MP2T H1QVGAH264 -
```

A transaction log file example triggered by Session Bitrate shift (Session Profile shifted) event looks like this:

```
10.140.8.24 hls 6a8-I-617F442F03277469298A3C17657B56C43529
http://hls.abr.com/sample/sample.m3u8 - 7368325 7837 bitrate_shift
[25/Sep/2012:11:11:59.998+0000] 67253471 96000 none cookie 200 "AppleCoreMedia/1.0.0.9B206
(iPad; U; CPU OS 5_1_1 like Mac OS X; zh_cn)" [25/Sep/2012:11:15:32.391+0000] video/MP2T
H2QVGAH264 -
```

A transaction log file example triggered by Session Bitrate shift event looks like this:

```
10.140.8.24 hls 6a8-I-617F442F03277469298A3C17657B56C43529
http://hls.abr.com/sample/sample.m3u8 - 7368325 7837 bitrate_shift
[25/Sep/2012:11:11:59.998+0000] 67253471 126000 none cookie 200
"AppleCoreMedia/1.0.0.9B206 (iPad; U; CPU OS 5_1_1 like Mac OS X; zh_cn)" "
[25/Sep/2012:11:15:32.391+0000] video/MP2T H1QVGAH264 -
```

A transaction log file example triggered by Session Stop event looks like this:

```
10.140.8.24 hls 6a8-I-617F442F03277469298A3C17657B56C43529
http://hls.abr.com/sample/sample.m3u8 - 6279214 6748 success
25/Sep/2012:11:15:59.895+0000] 56254582 300000 none cookie 200
"AppleCoreMedia/1.0.0.9B206 (iPad; U; CPU OS 5_1_1 like Mac OS X; zh_cn)" "
[25/Sep/2012:11:16:01.825+0000] video/MP2T H1QVGAH264 -
```

A transaction log file example triggered by Session Close event looks like this:

```
1 10.140.8.24 hls 6a8-I-617F442F03277469298A3C17657B56C43529
http://hls.abr.com/sample/sample.m3u8 - 0 0 close - 0 0 none cookie 200
"AppleCoreMedia/1.0.0.9B206 (iPad; U; CPU OS 5_1_1 like Mac OS X; zh_cn)" "
[25/Sep/2012:11:17:01.867+0000] video/MP2T - -
```

## Per Session Transaction Log Fields

[Table 8-56](#) describes the Per Session transaction log fields.

**Table 8-56 Per Session Transaction Log Fields**

Field	Description
client-ip	Client IP address.
abr-protocol	Type of session protocol.
session-id	Unique string generated by server to identify the session.
manifest-uri	URI of manifest file. If it is a failover session and the CDE does not receive request for master manifest file, this field is the asset URL (URL without asset filename).
asset-id	This field always returns a dash (-).
bytes-sent	Bytes sent to client. If this is session close log directly following a session stop, the field is 0 as nothing is sent since last log.
bytes-received	Bytes received from client. If the log entry consists of a session stop directly followed by a session close, the bytes-received field is 0.
status	Status of the session.

**Table 8-56 Per Session Transaction Log Fields (continued)**

Field	Description
time-received	If this is the first log entry for the transaction, it is the time stamp of when this session is received; otherwise, it is the time stamp of when the first HTTP transaction is received since last log message. If this is a session close log entry directly following a session stop log entry, the field is blank (-) because no request was received since last log.
time-to-serve	If this is the first log entry for the transaction, it is the time, in microseconds, taken since this session started; otherwise, it is the time when the first HTTP transaction is received since the last log message. If this is session stop log entry directly followed by a session stop, the field is 0.
bitrate	Current stream. A value of zero (0) means “not applicable” or “not available.” For HSS, the video bitrate is used as the overall stream bitrate.
encryption	Indicate the session encryption type.
session-tracking-mode	Method of tracking the session.
status-code	Status code added for not enough bandwidth (453) and not enough session (499).
user-agent	Description of client media player. All user-agent values are enclosed in double quotes (“ ”).
entry-gen-time	Time, in common log time format, that the log entry was generated.
mime-type	MIME type.
profile	The profile string retrieved from URL.
custom-parameter	Custom parameter retrieved from HTTP request URL or Session Cookie using the Service Rule:  <code>SessionCustomParameter#integer (RegEx)</code>

## Snapshot Counter Transaction Logs

The Snapshot Counter transaction logs for the SR and the SE record usage information per Delivery Service and can be sent to the CDNM for analytic reporting and billing purposes. For information on configuring the export of these transaction logs, see the [“Real-Time Exporting of Transaction Logs for Billing and Analytic Reports” section on page 8-102](#).

### Snapshot Counter Transaction Logs on SR for Session and Bandwidth

The SR Snapshot Counter transaction log records the session and bandwidth usage on the SEs in each Delivery Service. Each SE sends its own per-Delivery Service session and bandwidth counters in the keepalive messages to the SR. Once the SR receives this information, it aggregates the values across all the SEs in the Delivery Service. Every five seconds the SR writes a log entry to the Snapshot Counter transaction log.

The Snapshot Counter transaction log filename has the following format:

`sr_ds_counter_<ipaddr>_yyyymmdd_hhmmss_>`, where

- <ipaddr> represents the IP address of the SR
- yyyymmdd\_hhmmss represents the date and time when the log was created

The Snapshot Counter transaction log file is located in the /local/local1/logs/ds\_snapshot\_counter/ directory on the SR.

[Table 57](#) describes the fields for the Snapshot Counter transaction log.

**Table 57 SR Snapshot Counter Transaction Log Fields**

Field	Description
time	Time, in common log time format, the per-Delivery Service counters were generated on the SE.
se-name	Name of the SE. A value of “–” means the log entry is aggregated for the Delivery Service.
ds-id	Delivery service ID with “Channel_” as the prefix string.
active-sessions	Number of active sessions for the Delivery Service.
allocated-bandwidth	Average allocated bandwidth (in kilo bits per second) for the active sessions.

### Snapshot Counter Transaction Logs on SE for Storage Usage

The SE Snapshot Counter transaction log on the SE records the storage usage for prefetched content and dynamically cached content. Every 30 seconds the SE writes a log entry to the Snapshot Counter transaction log to record the per-Delivery Service storage usage.

The snapshot counter transaction log filename has the following format:

se\_ds\_counter\_<ipaddr>\_yyyymmdd\_hhmmss\_<>, where

- <ipaddr> represents the IP address of the SE
- yyyymmdd\_hhmmss represents the date and time when the log was created

The Snapshot Counter transaction log file is located in the /local/local1/logs/ds\_snapshot\_counter/ directory on the SE.

[Table 58](#) describes the fields for the Snapshot Counter transaction log.

**Table 58 SE Snapshot Counter Transaction Log Fields**

Field	Description
time	Time, in common log time format, the per-Delivery Service counters were generated on the SE.
se-name	Name of the SE.
ds-id	Delivery service ID with “Channel_” as the prefix string.
storage-quota-usage-prep	Amount of storage used (in bytes) for prefetched content.
storage-quota-usage-dynamic	Amount of storage used (in bytes) for dynamically ingested content.

### URL Snapshot Counter Transaction Logs on SE for Delivery Service Monitoring Active TCP Sessions

The url snapshot counter transaction log file name has the following format:

we\_url\_counter\_[ipaddr]\_yyyymmdd\_hhmmss\_[index], where

- [ipaddr] represents the IP address of the SE
- yyyymmdd\_hhmmss represents the date and time when the log was created

**Transaction Logs**

The url snapshot transaction log file is located under directory /local/local1/logs/webengine\_url\_snapshot\_counter/ named we\_url\_counter on the SE.

[Table 59](#) describes the fields for the Snapshot Counter transaction log.

**Table 59 Web Engine URL Snapshot Counter Transaction Log Fields**

Field	Description
time	Time, in common log time format, the per-Delivery Service counters were generated on the SE.
ds-id	Delivery service ID with “Channel_” as the prefix string.
regex-url	The regex url matched in the rule file.
request-url	Requested URL, if query string is required by the rule file, it will include the query string otherwise it doesn't include the query string.
active-sessions	Number of active sessions belongs the Delivery Service.
bytes-sent	Number of bytes sent since the previous snapshot.
allocated-bandwidth	Average allocated bandwidth (in kilo bits per second from the SE to the End User) for the active sessions.
http-requests	Number of HTTP requests received since the previous snapshot.

### Enabling the Snapshot Counter Transaction Log

The per-Delivery Service snapshot counter transaction log is disabled by default. To enable the per-Delivery Service snapshot counter transaction log function of a device, use the Transaction Logging page for the SE and the SR. For an SE, choose **Devices > Devices > Service Control > Transaction Logging**. For an SR, choose **Devices > Devices > General Settings > Notification and Tracking > Transaction Logging**.

### Real-Time Exporting of Transaction Logs for Billing and Analytic Reports

Transaction logs can be sent real-time from the SE and SR to the CDNM or other export server for use in analytic reports, summary billing records, and detailed transaction records on a per-Delivery Service basis. The SE and SR use the Splunk Universal Forwarder (UF) to push the transaction logs to the Splunk Lightweight Forwarder (LWF) on the CDNM.



**Note** The export server, whether the CDNM, other CDN, or different server; must have the Splunk LWF running and configured to receive the transaction log files.

These log files can be opened with a text editor, saved to a local hard drive, and used to generate monthly reports of charges for delivered content for each content provider.

To configure the real-time exporting of the transaction logs, use the Transaction Logging page for the SE and the SR. For an SE, choose **Devices > Devices > Service Control > Transaction Logging**. For an SR, choose **Devices > Devices > General Settings > Notification and Tracking > Transaction Logging**.



# Maintaining the Videoscape Distribution Suite, Internet Streamer

---

This chapter explains how to perform common administrative tasks including updating system software, hard disk drive maintenance, and rebooting and deleting devices. The following major topics are covered:

- [Software Upgrade, page 9-1](#)
- [Rebooting Devices, page 9-10](#)
- [Deleting a Device, page 9-10](#)
- [Replacing a Device, page 9-13](#)
- [Backup and Recovery Procedures, page 9-16](#)
- [Disk Maintenance, page 9-27](#)

For information about database maintenance, see the “[Scheduling Database Maintenance](#)” section on [page 4-60](#).

## Software Upgrade

The software upgrade section covers the following topics:

- [Getting a Software File from Cisco.com](#)
- [Finding the Software Version of the Devices](#)
- [Configuring the Software Image Settings](#)
- [Upgrading the Software](#)
- [Software Upgrades by Device](#)

## Getting a Software File from Cisco.com

To get a software file from Cisco.com, follow these steps:

- 
- Step 1** Launch your web browser and enter the following URL:  
<http://www.cisco.com/cisco/software/navigator.html>

The Select a Product page is displayed if you have recently logged in; otherwise, the Log In page is displayed.

- Step 2** Log in to Cisco.com using your designated username and password. The Video and Content Delivery page is displayed, listing the available software products.
  - Step 3** Choose **Products > Video and Content Delivery > Content Delivery Systems > Content Delivery Applications > Cisco Internet Streamer Application**. The Downloads page is displayed.
  - Step 4** Click the software release you want. The page refreshes and the software image files are displayed.
  - Step 5** Click the link for the software image file you want.
    - If this is the first time you have downloaded a file from Cisco.com, the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy is displayed. Read the policy, fill in the unfilled fields, and click **Accept**.
    - If you previously filled out the Encryption Software Usage and Handling and Distribution form, the form does not display again.
- The Download page is displayed with the information about the software image file and a Download link.
- Step 6** Click **Download Now** to download the file, or click **Add to cart** to select more image files before downloading them. The Download Cart page is displayed.
  - Step 7** Click **Proceed With Download**. The Cisco End User Software License Agreement is displayed.
  - Step 8** Read the agreement and click **Agree**. The Download Software page is displayed.
  - Step 9** Choose a download option, either **Download Manger Option** or **Non Java Download Option**. A new window displays the filename of the ISO image file.
  - Step 10** Click **Download**. The File Download dialog box is displayed.
  - Step 11** Click **Save**. The Save As dialog box is displayed.
  - Step 12** Navigate to the location where you want to save the file and click **Save**. The file downloads.

## Pre-positioning a Software File

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 5, “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.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).

## Finding the Software Version of the Devices

The CDSM Home page gives a brief summary of the software versions in use on all the devices in the Videoscape Distribution Suite, Internet Streamer (VDS-IS) 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.

**Note**

The software version is not upgraded until a software upgrade has been successfully completed. If a software upgrade is in progress, the version number displayed is the base version, not the upgraded version number.

## Configuring the Software Image Settings

To upgrade your VDS-IS software release, you must first configure the software image settings.

To configure the software image settings, follow these steps:

- 
- 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 9-1](#)).

**Software Upgrade****Figure 9-1 Software Image Page**

The screenshot shows the 'Creating New Software Image' page. At the top, there's a navigation bar with tabs for Devices, Services, System, and Software Image Management. The Software Image Management tab is selected. Below the tabs, there's a breadcrumb trail: AAA > Password > Logs > Configuration > Software Image Management. The main form has several sections:

- Software Image Settings:** Contains fields for Software Image URL (set to 'ftp://'), Username, Password, Confirm Password, Software Version (example: 2.0.0.b.70), and File Size (bytes).
- Advanced Settings:** Contains options for Auto Reload (checked), Download Method (Default selected), and CDSM IP Address.
- Comments:** A text area for additional notes.

A 'Validate Software Image Settings' button is located between the two main sections. The bottom right corner of the page displays the number '211837'.

**Step 3** In the **Software Image URL** field, enter the URL for the .bin software file that you downloaded from Cisco.com.

- Choose a protocol (**http** or **ftp**) from the drop-down list.
- Enter the URL of the software file; for example, a valid URL might look like this:  
`http://internal.mysite.com/cds/CDS-2.x.x-K9.bin`

In this URL, *CDS-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 a Software File” section on page 9-2 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 a Software File” section on page 9-2.)

**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 a CDSM 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 **CDSM IP address** field.

The CDSM IP address field is the IP address of a CDSM after the software is downgraded. (This field is optional and only applies for downgrades.) After the downgrade, the SE registers with the CDSM 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 CDSM, 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 CDSM. 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 9-6.)

## Upgrading the Software

When upgrading software in your VDS-IS network, begin with Service Engines and Service Routers before upgrading the CDSM. The CDSM reboots at the conclusion of the upgrade procedure, causing you to temporarily lose contact with the device and the user interface. After the CDSM has upgraded its software and rebooted, it may be unable to communicate with devices running different versions of the VDS-IS software.



### Caution

Primary and standby CDSMs must be running the same version of VDS-IS software. If they are not, the standby CDSM detects this and does not process any configuration updates it receives from the primary CDSM. You need to upgrade your standby CDSM first, and then upgrade your primary CDSM. We also recommend that you create a database backup for the primary CDSM and copy the database backup file to a safe place before you upgrade the software.



### 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 4-6 on page 4-11](#) for more information.

## Downgrading the Software

For software downgrades of systems with primary and standby CDSMs, you need to follow these steps:

1. If you are using the CDSM GUI, downgrade the standby CDSM first, followed by the primary CDSM.  
If you are using the CLI, downgrade the primary CDSM first, followed by the standby CDSM.
2. After downgrading the primary and standby CDSMs, using the CLI, log in to each CDSM and run the following commands:

```
cms database downgrade
cms enable
```

3. Downgrade the software on the Service Routers.
4. Downgrade the Content Acquirers.
5. Downgrade the middle-tier Service Engines.
6. Downgrade the edge Service Engines.



### Note

Before downgrading from Release 4.0 to the previous 3.x release image, you need to execute the content-mgr rollback command on the Service Engine, otherwise all the cached content will be lost after downgrade. The content-mgr rollback command evicts the cached disk content till max cached files count below 20,000,000 and max cached directories count below 950,000.

## Interoperability Considerations

In general, a VDS-IS 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:

- VDS-IS 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 VDS-IS 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 VDS-IS network devices in the following order:

1. Multicast sender Service Engines
2. Multicast receiver Service Engines
3. Edge Service Engines
4. Middle-tier Service Engines
5. Content Acquirers



**Note**

---

When upgrading the Content Acquirers in a Delivery Service, to avoid having a critical alarm generated while the Content Acquirer is being upgraded, temporarily set the System.datafeed.pollRate field to 200 seconds or higher. When the upgrade is complete, reset the field to the original value. See the “[System Properties](#)” section on page 6-8 for more information.

---

6. Service Routers
7. Standby CDSMs (Upgrade before primary when using the GUI only.)
8. Primary CDSM



**Note**

---

When you upgrade CDSMs using the CLI, we recommend that you upgrade your primary CDSM first, and then upgrade your standby CDSM. Primary and standby CDSMs must be operating with exactly the same software release as each other for failover to be successful.

---

## Upgrading Software by Device Groups



**Note**

---

This procedure is for Service Engines only. Service Routers and CDSMs cannot be associated with device groups.

---

To upgrade your software on multiple Service Engines, follow these steps:

- 
- 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 9-1](#) for a description of upgrade status messages.

---

**Table 9-1 Upgrade Status Messages**

Upgrade Status Message	Condition
Pending	The request has yet to be sent from the CDSM 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.
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.

**Table 9-1 Upgrade Status Messages (continued)**

Upgrade Status Message	Condition
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

Use this upgrade procedure for Service Routers and CDSMs. You can also use this upgrade procedure to upgrade Service Engines one at a time.

To upgrade your software on a single device, follow these steps:

- 
- 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 9-1](#) for a description of upgrade status messages.



- 
- Note** For a Service Engine with physical memory less than 32GB, if the cached file entries is less than 16 million, the Content Manager will run with the max-cached-entries value of 16 million after upgrading the software image to 4.0. If the cached file entries is greater than 16 million, the Content Manager runs with the max-cached-entries value of 20 million after upgrading the software image to 4.0.
-

## Rebooting Devices

You can reboot a device or device group. The CDSM performs a controlled shutdown of all devices and then restarts the operating system on each device.

To reboot an individual device, follow these steps:

- 
- 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**.
- 

To reboot an entire device group, follow these steps:

- 
- 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 VDS-IS network using its new address and configuration information.



- Caution** If you delete the only SR in your VDS-IS network, you are removing the ability of your VDS-IS network to fill user requests.

When you delete an SE from the VDS-IS network, you are removing that device and the content it contains from the routing scheme that the VDS-IS uses to fill user requests. Although the VDS-IS routes requests around SEs that are busy, offline, or missing, removing an SE may affect the speed at which the VDS-IS 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 VDS-IS network involves using the CLI to shut down VDS-IS 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 CDSM; 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 VDS-IS network, the following conditions must be met:

- Device must have been activated in the CDSM.
- CDSM must be operating.
- Device must have the correct CDSM IP address or hostname configured.
- CDSM IP address or hostname must be that of the primary CDSM.
- Device must not be the Content Acquirer for any Delivery Service.

Deleting a device from the VDS-IS network involves using the CLI to remove the registration information from the device itself and removing the registration record from the CDSM.

**Note**

Do not use the CDSM to delete a device while the device is still active and registered. The CDSM delete feature removes only the device's registration record from the CDSM; it does not deregister the device. The device retains its registration information and continues to contact the CDSM; however, the CDSM no longer recognizes the device.

If for some reason the CDSM 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 CDSM as though it were a new node in the VDS-IS network.

To remove and deregister a device, follow these steps:

**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
```

**■ Deleting a Device****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 CDSM or registering the device to another CDSM. The **cms deregister force** command forces the deregistration to continue.

- 
- Step 5** To add the device back into the VDS-IS network, reregister the device with the CDSM by using the **cms enable** command in global configuration mode.

```
SE# configure
SE(config)# cms enable
```

---

In case of a hardware failure, you might need to remove the device from the VDS-IS network routing scheme by using the CDSM.

Before a device can be removed from the VDS-IS network through the CDSM, the following conditions must be met:

- Device must have been activated in the CDSM.
- CDSM must be running.
- Device must have the correct CDSM IP address or hostname configured.
- CDSM IP address or hostname must point to the primary CDSM.
- Device must not be the Content Acquirer for any Delivery Service.

To delete a device using the CDSM, follow these steps:

- 
- 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 CDSM.
- 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 CDSM. This is because once the device has been deleted, the CDSM no longer has a record of the device.

- Step 7** To add the device back in to the VDS-IS network, reregister the device with the CDSM by using the **cms enable** command in global configuration mode.

## Deleting a Warm Standby CDSM

You can delete a warm standby CDSM from the VDS-IS network at any point after you have registered the device and before the device has come online as the primary CDSM. Once the device has been called into use as the primary CDSM, however, you cannot delete it by using the CDSM.

Delete a warm standby CDSM 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 VDS-IS network by using its new address and configuration information.

To delete a warm standby CDSM, follow these steps:

- Step 1** Log in directly to the CDSM 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 CDSM GUI, choose **Devices > Devices**.  
The browser refreshes, listing the CDSMs on your VDS-IS network. The warm standby CDSM is identified as *Standby*.
- Step 3** Click the **Edit** icon next to the name of the warm standby CDSM. 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 VDS-IS is different depending on the type of the device being replaced. This section covers the following procedures:

- [Replacing a CDSM](#)
- [Replacing an SE or SR](#)

## Replacing a CDSM

To replace a CDSM in a VDS-IS you must first add the new CDSM into the network as a standby CDSM. For procedural information, see the “[Configuring Primary and Standby CDSMs](#)” section on page 3-11.

**Note**

The primary and standby CDSMs must be running the same version of software. You must first add the new CDSM with the same version as the existing CDSM. Once the standby CDSM 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 CDSM using the primary CDSM 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 CDSM has a record of the most recent configuration changes.

To promote the standby CDSM to primary, first stop the primary CDSM using the **cdsm role standby** command. For procedural information, see the “[Changing a Standby CDSM to a Primary CDSM](#)” section on page 3-12.

After the primary CDSM has been stopped, and the standby CDSM has taken the role of primary, wait at least two polling intervals (10 minutes) before logging in to the new primary CDSM. The new primary CDSM is accessible by entering the IP address of the CDSM with port 8443 in a web browser. For example, if the IP address of your CDSM is 192.168.0.236, enter **https://192.168.0.236:8443**.

It is now safe to deactivate the old primary CDSM in the CDSM web interface and remove it from the VDS-IS network.

**Note**

Do not try to take a back up of the old CDSM database and restore it on the new CDSM. 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, follow these steps:

---

**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 CDSM, 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.devicve.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 *Cisco Content Delivery Engine Hardware Installation Guide* that is applicable to your device.



**Note** The replacement device must be the same hardware model as that of the device being replaced.

- When prompted by the setup utility, configure the basic network settings.
- 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.”
- When prompted by the setup utility for the IP address of the CDSM, enter the IP address of the CDSM.

- 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 CDSM, 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 CDSM by using the **cms enable** command in global configuration mode.

```
SE# configure
SE(config)# cms enable
```

- Step 13** From the CDSM, 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 VDS-IS network.

# Backup and Recovery Procedures

This section provides CDSM database backup and VDS-IS software recovery procedures. This section contains the following sections:

- [Performing Backup and Restore on the CDSM Database, page 9-16](#)
- [Using the Cisco VDS-IS Software Recovery CD-ROM, page 9-17](#)
- [Recovering the System Software, page 9-19](#)
- [Recovering a Lost Administrator Password, page 9-22](#)
- [Recovering from Missing Disk-Based Software, page 9-23](#)
- [Recovering VDS-IS Network Device Registration Information, page 9-25](#)

## Performing Backup and Restore on the CDSM Database

The CDSM stores VDS-IS 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 CDSM, 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 CDSM, follow these steps:

---

**Step 1** Back up the CMS database to a file.

```
CDE# 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:

```
CDE# cd /local/local1
CDE# 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-3.0.1-18) 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.

```
CDE# cms database delete
```

- Step 4** Restore the CMS database contents from the backup file.

```
CDE# cms database restore cds-db-9-22-2002-17-36
```

- Step 5** Enable CMS.

```
CDE# cms enable
```

## Using the Cisco VDS-IS Software Recovery CD-ROM

A software recovery CD-ROM image (.iso file) is available for each software release. The recovery CD-ROM can be used to recover system software that must be completely reimaged. The recovery CD-ROM image contains the system software for a single software release and a single application software.

This section presents instructions for creating and using the software recovery CD-ROM to reinstall your system software if for some reason the software that is installed has failed.



**Caution**

If you upgraded your software with a later release than the software recovery CD-ROM image file you downloaded, using the CD-ROM software recovery images may downgrade your system.

## System Software Components

Cisco VDS-IS software consists of three basic components:

- Disk-based software
- Flash-based software
- Hardware platform cookie (stored in flash memory)

All these components must be correctly installed for Cisco VDS-IS software to work properly.

The software is contained in two types of software images provided by Cisco:

- A .bin image containing disk and flash memory components

An installation containing only the VDS-IS flash memory-based software, without the corresponding disk-based software, boots and operates in a limited mode, allowing for further disk configuration before completing a full installation.

- A .sysimg image containing a flash memory component only

The .sysimg component is provided for recovery purposes, and allows for repair of flash memory only, without modifying the disk contents.

## Getting the Cisco VDS-IS Software Recovery File from Cisco.com

To get a software file from Cisco.com, follow these steps:

- 
- Step 1** Launch your web browser and enter the following URL:  
<http://www.cisco.com/kobayashi/sw-center/sw-video.shtml>  
The Log In page is displayed.
- Step 2** Log in to Cisco.com using your designated username and password. The Video and Content Delivery page is displayed, listing the available software products.
- Step 3** Click **Cisco Content Delivery Systems (CDS)**. The Downloads page is displayed.
- Step 4** Click the **Cisco Content Delivery Applications** folder to expand it, and click the **Cisco Internet Streamer Application**. The page refreshes and the software releases are displayed.
- Step 5** Click the link for the software recovery file you want to download.
- If this is the first time you have downloaded a file from Cisco.com, the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy is displayed. Read the policy, fill in the unfilled fields, and click **Accept**.
  - If you previously filled out the Encryption Software Usage and Handling and Distribution form, the form does not display again.
- The Download page is displayed with the information about the software image file and a Download link.
- Step 6** Click **Download**. The Cisco End User Software License Agreement is displayed.
- Step 7** Read the agreement and click **Agree**. The File Download dialog box is displayed.
- Step 8** Click **Save**. The Save As dialog box is displayed.
- Step 9** Navigate to the location where you want to save the file and click **Save**. The file downloads.
- Step 10** Burn the software recovery image file onto a CD-ROM.
- 

## Installing the Software Using the Recovery CD-ROM

To install the system software by using the recovery CD-ROM, perform the following steps:

- 
- Step 1** Plug a USB CD-ROM drive into a USB port on the device.
- Step 2** Insert the recovery software CD-ROM into the USB CD-ROM drive, and boot the device.
- Step 3** When the installer menu appears, choose **2 Install all Software**.
- Step 4** Wait for the process to complete.
- Step 5** Before you reboot the device, remove the USB CD-ROM drive from the USB port so that the device boots from flash memory.
- Step 6** Reboot the device.
-

## Recovering the System Software

The Service Engine, Service Router, and CDSM have a resident rescue system image that is invoked should the image in flash memory be corrupted. A corrupted system image can result from a power failure that occurs while a system image is being written to flash memory. The rescue image can download a system image to the main memory of the device and write it to flash memory.

**Note**

The .sysimg file is located under the images folder on the Recovery CD-ROM. If you have upgraded the VDS-IS software, download the corresponding rescue CD iso image, copy to a CD and use the rescue iso image.

To install a new system image using the rescue image, follow these steps:

- 
- Step 1** Download the system image file (\*.sysimg) to a host that is running an FTP server.
  - Step 2** Establish a console connection to the device and open a terminal session.
  - Step 3** Reboot the device by toggling the power switch.

The rescue image dialog appears. The following example demonstrates how to interact with the rescue dialog and use a port channel for the network connection (user input is denoted by entries in bold typeface). This example is for the CDE220-2G2, which has 10 gigabit Ethernet interfaces. The CDE110 and CDE205 have 2 gigabit Ethernet interfaces and the has 14 gigabit Ethernet interfaces.

This is the rescue image. The purpose of this software is to let you download and install a new system image onto your system's boot flash device. This software has been invoked either manually (if you entered `\*\*\*` to the bootloader prompt) or has been invoked by the bootloader if it discovered that your system image in flash had been corrupted.

To download an image, this software will request the following information from you:

- which network interface to use
- IP address and netmask for the selected interface
- default gateway IP address
- FTP server IP address
- username/password on FTP server
- path to system image on server

System Recovery Menu:  
1. Configure Network  
2. Download and install system image  
3. Exit (and reboot)  
Choice [1]: 1

Network Configuration Menu:  
1. Configure ethernet interface  
2. Configure portchannel interface  
3. Exit to main menu  
Choice [1]: 2

Please enter an interface from the following list:  
0. GigabitEthernet 1/0  
1. GigabitEthernet 2/0  
2. GigabitEthernet 3/0  
3. GigabitEthernet 4/0  
4. GigabitEthernet 5/0  
5. GigabitEthernet 6/0

**■ Backup and Recovery Procedures**

```

6. GigabitEthernet 7/0
7. GigabitEthernet 8/0
8. GigabitEthernet 9/0
9. GigabitEthernet 10/0
10. Done
0
Please select an interface from the list below:
0. GigabitEthernet 1/0 [Use]
1. GigabitEthernet 2/0
2. GigabitEthernet 3/0
3. GigabitEthernet 4/0
4. GigabitEthernet 5/0
5. GigabitEthernet 6/0
6. GigabitEthernet 7/0
7. GigabitEthernet 8/0
8. GigabitEthernet 9/0
9. GigabitEthernet 10/0
10. Done
Choice [1]: 1

Please select an interface from the list below:
0. GigabitEthernet 1/0 [Use]
1. GigabitEthernet 2/0 [Use]
2. GigabitEthernet 3/0
3. GigabitEthernet 4/0
4. GigabitEthernet 5/0
5. GigabitEthernet 6/0
6. GigabitEthernet 7/0
7. GigabitEthernet 8/0
8. GigabitEthernet 9/0
9. GigabitEthernet 10/0
10. Done
Choice [2]: 10

Please enter the local IP address to use for this interface:
[Enter IP address]: 172.16.22.22

Please enter the netmask for this interface:
[Enter Netmask]: 255.255.255.224

Please enter the IP address for the default gateway:
[Enter Gateway IP address]: 172.16.22.1

Network Configuration Menu:
1. Configure ethernet interface
2. Configure portchannel interface (done)
3. Exit to main menu
Choice [3]: 3

System Recovery Menu:
1. Configure Network (done)
2. Download and install system image
3. Exit (and reboot)
Choice [2]: 2

Please enter the IP address for the FTP server where you wish
to obtain the new system image:
[Enter Server IP address]: 172.16.10.10

Please enter your username on the FTP server (or 'anonymous'):
[Enter Username on server (e.g. anonymous)]: anonymous

Please enter the password for username 'anonymous' on FTP server (an email address):

```

Please enter the directory containing the image file on the FTP server:  
 [Enter Directory on server (e.g. /)]: /

Please enter the file name of the system image file on the FTP server:  
 [Enter Filename on server]: **CDS24.sysimg**

Here is the configuration you have entered:

Current config:

```
IP address: 172.16.22.22
Netmask: 255.255.255.224
Gateway Address: 172.16.22.1
Server Address: 172.16.10.10
Username: anonymous
Password:
Image directory: /
Image filename: CDS-24.sysimg
```

Attempting download...

Downloaded 34234368 byte image file

A new system image has been downloaded.

You should write it to flash at this time.

Please enter 'yes' below to indicate that this is what you want to do:

[Enter confirmation ('yes' or 'no')]: **yes**

Ok, writing new image to flash

.....Finished  
writing image to flash.

Enter 'reboot' to reboot, or 'again' to download and install a new image:

[Enter reboot confirmation ('reboot' or 'again')]: **reboot**

Restarting system.

Initializing memory. Please wait.

System Recovery Menu:

1. Configure Network (done)
2. Download and install system image (done)
3. Exit (and reboot)

Choice [3]: **3**

Restarting system.

**Step 4** Log in to the device as username **admin**. Verify that you are running the correct version by entering the **show version** command.

Username: **admin**

Password:

Console> **enable**

Console# **show version**

Content Delivery System Software (CDS)

Copyright (c) 2007 by Cisco Systems, Inc.

Content Delivery System Software Release 3.0.0 (build b460 July 5 2011)

Version: se507-2.4.0

Compiled 02:34:38 July 15 2009 by (cisco)

Compile Time Options: PP SS

System was restarted on Thu July 15 16:03:51 2009.

The system has been up for 4 weeks, 1 day, 6 hours, 7 minutes, 23 seconds.

## Recovering a Lost Administrator Password

If an administrator password is forgotten, lost, or mis-configured, you need to 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, follow these steps:

**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 VDS-IS software, the bootflags are reset to 0x0 on every reboot.

## Recovering from Missing Disk-Based Software

This section describes the recovery procedures to use if for some reason the software installation on both system disks is corrupt or missing.

There are two types of disk volumes in the VDS-IS: system disk volumes (which contain all of the system volumes plus the sysfs volume) and cdnfs disk volumes. A disk is either allocated as a system disk or a cdnfs disk (on some CDEs, a system disk might contain a cdnfs volume). The system volumes, contain data and applications that are critical to the system's basic functionality.

The system volumes are stored in a two-disk RAID-1 (mirrored) array. RAID-1 duplicates data between each of the disks in the array. The two-disk scheme allows for either of the drives in the system volumes array to fail without sustaining data loss or incurring system errors.

The status of the volumes can be seen through the **show disk raid-state** command, and can be in any of the following states:

- Normal—Both drives are attached, and data is mirrored between them.
- Syncing—Data is being copied between the drives to restore the volumes to a normal state. This typically happens when a new drive is added to repair degraded volumes.
- Degraded—One of the disks has failed. It is highly recommended that a new disk is added to repair the volumes.
- Bad—Both disks have failed. The system has likely lost all but basic functionality.



- Note**

If both system disks fail, a VDS-IS state of “missing disk-based software” occurs.

Normally, when a problem occurs on one system disk, a disk failure or RAID alarm is triggered. If this occurs, replace the failed disk. See the “[Disk Maintenance](#)” section on page 9-27.

The VDS-IS state of “missing disk-based software” is most likely to occur if you replaced both system disks in your Service Engine, Service Router, or CDSM. By design, the software installation on the system disks cannot be corrupted by a system failure or a power failure.

If both system disks fail or are missing, the software continues to run. However, it runs in a basic functionality mode in which HTTP proxy and related HTTP features still work, but most other features fail.

The compact flash functionality is merged on to the system disk in a non-CDE platform. If both system disks fail or are missing on a non-CDE platform, the non-CDE device can not function and needs to have the VDS-IS software reinstalled by using the Recovery CD-ROM. For more information, see the “[Using the Cisco VDS-IS Software Recovery CD-ROM](#)” section on page 9-17.

**■ Backup and Recovery Procedures****Caution**

This procedure should only be used as a last-resort method to recover the system software on a unit. Typically, the system automatically repairs itself across a reboot if any new disks are detected. If the volumes are degraded and a new disk is present at reboot, the new disk is added to the existing array (sync starts). If the volumes are “bad” and a new disk is present at reboot, the initial system volume is built on the disk.

To recover from this condition, follow these steps:

**Step 1** Remove the Service Engine record from the CDSM.

- a. Choose **Devices > Devices**.
- b. Click the **Edit** icon next to the name of the Service Engine that you want to delete. The Devices home page is displayed.
- c. Click the **Delete** icon. You are prompted to confirm your decision.
- d. Click **OK** to execute your request. The Service Engine is removed from the CDSM.

**Note**

The Service Engine registration record needs to be deleted from the CDSM for the Service Engine to complete reregistration after it comes back online. The CDSM does not register a device if the device already appears in the record as registered.

**Step 2** Power down the device and replace the failed or missing system disks with new, blank disks.**Step 3** After the new disks are installed, power up the device.**Step 4** From a console or through an SSH session, check the startup messages that appear on your screen.

If there is a problem with the system disk or the disk-based software, a message similar to the following appears:

```
Jan 21 21:55:45 (none) ruby_disk:%SE-DISK-2-200024:First disk not in standard
configuration. Run 'disk recover-system-volumes' command and re-install software.
ruby_disk:Your first disk is not in standard configuration.
ruby_disk:Run 'disk recover-system-volumes' from the CLI
```

```
*****
System software is missing.
Check whether first-disk is bad, or
use 'disk recover-system-volumes' to recover first-disk.
*****
```

**Step 5** Log in as **admin**.

```
Cisco Service Engine Console
```

```
Username: admin
Password:
System Initialization Finished.
```

```
SE-507 con now available
```

```
Press RETURN to get started!
```

**Step 6** After logging in to a console or SSH session, enter the **copy ftp install** or **copy http install** EXEC command to download and install a new system image.

```
ServiceEngine# copy ftp install ftp-server remotefiledir remotefilename
```

For example:

- Step 7** Reboot the software with the new disk and new system image by entering the **reload EXEC** command.

SE# **reload**

- Step 8** Register the device with the CDSM by using the **cms enable** command in global configuration mode.

```
SE# configure  
SE(config)# cms enable
```

## Recovering VDS-IS Network Device Registration Information

Device registration information is stored both on the device itself and on the CDSM. If a device loses its registration identity or needs to be replaced because of hardware failure, the VDS-IS 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, follow these steps:

- Step 1** Mark the failed device as “Inactive” and “Replaceable” in the CDSM.

  - Choose **Devices > Devices**.
  - Click the **Edit** icon next to the name of the Service Engine you want to deactivate. The Devices home page is displayed.
  - From the left-panel menu, choose **Device Activation**.
  - 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.
- Choose **System > Configuration**.
  - Click the **Edit** icon next to the System.device.recovery.key property. The Modifying Config Property page is displayed.
  - 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 CDSM.

When the CDSM 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 CDSM 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 CDSM and activate the device.
- Choose **Devices > Devices**.
  - Click the **Edit** icon next to the name of the Service Engine you want to activate. The Devices home page is displayed.
  - From the left-panel menu, choose **Device Activation**. The Service Engine status should be Online.
  - Check the **Activate** check box and click **Submit**.



**Note** If you are replacing an old device with a different hardware model, check the following hardware-related settings and adjust them according to your needs, after the new device is online in CDSM GUI:

- IP Access List settings associated with network interfaces
- Disk quota settings of VOD-type delivery services
- Default and maximum bandwidth setting of Windows Media Streaming and Movie Streamer
- Service Monitor Disk Failure Percent Settings

# Disk Maintenance

This section covers the following topics:

- [Disk Error Handling](#)
- [Removing and Replacing Disk Drives](#)

## Disk Error Handling

When sector I/O errors on a disk exceed the Disk Error Handling Thresholds, the disk is marked bad. The following tasks are performed when a disk is marked bad:

- Raise a disk\_failure alarm
- Forcibly unmount the disk
- Inform the CAL/UNS layer of any CDNFS partitions that are marked bad so that they cannot be used for streaming (CDNFS partitions only)
- Intentionally invalidate the Master Boot Record (MBR) of the disk, thereby destroying any cached content. This eliminates the possibility of reusing potentially corrupt cached content. This essentially removes the disk from the CDNFS file-system.

The disk must be repaired before it can be reused by the VDS-IS system software.

For information about disk error handling thresholds, see the “[Enabling Disk Error Handling](#)” section on page 4-61.

The following sections cover detecting disk sector errors and repairing them:

- [Disk Latent Sector Error Handling](#)
- [SMART Sector Errors](#)
- [disk repair Command](#)

## 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 when there are disk sector errors:

```
Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-4-900000: end_request: I/O error, dev sdd,
sector 4660
Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-3-900000: Buffer I/O error on device sdd,
logical block 582
```

## SMART Sector Errors

Typically, the indication that a hard disk drive (HDD) is bad and needs to be replaced is if the **show disk SMART-info detail** command output exceeds the values described in [Table 9-2](#). Solid State Drives (SSDs) do not report pending errored sector attributes in the output for the **show disk SMART-info detail** command.

**Table 9-2 Output Values of show disk SMART-info detail Command Indicating Disk Replacement**

Field	CDNFS and SYSTEM Drives—Threshold Raw Values
Reallocated_Sector_Ct raw_value	128
Current_Pending_Sector raw_value	30
Offline_Uncorrectable raw_value	30

A drive needs to be replaced if any of the RAW\_VALUES listed in [Table 9-2](#) are exceeded.

The **show disk SMART-info** command (without the **detail** keyword), provides information on the overall health of each HDD or SSD. The following example of the **show disk SMART-info** command output shows that disk08 is bad:

```
# show disk SMART-info

... etc ...

==== disk08 ====
smartctl 5.40 2010-10-16 r3189 [i686-pc-linux-gnu] (local build)
Copyright (C) 2002-10 by Bruce Allen, http://smartmontools.sourceforge.net

==== START OF INFORMATION SECTION ====
Model Family:      Seagate Barracuda ES.2
Device Model:     ST3500320NS
Serial Number:    9QM92HZ0
Firmware Version: SN05
User Capacity:    500,107,862,016 bytes
Device is:        In smartctl database [for details use: -P show]
ATA Version is:   8
ATA Standard is: ATA-8-ACS revision 4
Local Time is:    Tue Jul 19 04:42:16 2011 PDT

==> WARNING: There are known problems with these drives,
see the following Seagate web pages:
http://seagate.custkb.com/seagate/crm/selfservice/search.jsp?DocId=207931
http://seagate.custkb.com/seagate/crm/selfservice/search.jsp?DocId=207963

SMART support is: Available - device has SMART capability.
SMART support is: Enabled

==== START OF READ SMART DATA SECTION ====
SMART overall-health self-assessment test result: FAILED!
Drive failure expected in less than 24 hours. SAVE ALL DATA.
Failed Attributes:
ID# ATTRIBUTE_NAME      FLAG     VALUE  WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
  5 Reallocated_Sector_Ct  0x0033  025    025    036    Pre-fail  Always   FAILING_Now 1548
```

The **show disk SMART-info** command is repeated for each drive. If the overall-health assessment of a drive indicates “FAILED,” then the drive should be replaced. The output of the **show disk SMART-info** command also shows the SMART attributes that indicate drive failure (in the above example, the **Reallocated\_Sector\_Ct** attribute indicates FAILING\_NOW).

If the **show disk SMART-info details** command output values for Current\_Pending\_Sector and Offline\_Uncorrectable for an HDD are below the threshold described in [Table 9-2](#), then monitor these values over several days. The Latent Sector Error feature attempts to repair such errored sectors in a background process by deleting (evicting) corrupted content. If after several days of monitoring the values for Current\_Pending\_Sector and Offline\_Uncorrectable have not decreased, consider running the **disk repair** command. After the **disk repair** command completes, we recommend that you reboot the SE to ensure all VDS-IS software services are functioning correctly.

If the output values for Current\_Pending\_Sector and Offline\_Uncorrectable for an HDD are above the threshold described in [Table 9-2](#), then you need to replace the disk.



**Note** The **disk repair** command deletes all cached video content on the drive and takes approximately three hours to complete per HDD. The **disk repair** command takes approximately 30 minutes on a solid-state drive (SSD).

[Table 9-3](#) provides an example of the last part of the output of the **show disk SMART-info detail** command. The attributes that need to be reviewed to determine if the drive needs to be replaced or repaired are highlighted in bold. A drive needs to be replaced if any of the RAW\_VALUES listed in [Table 9-2](#) are exceeded. In this example, because the **Reallocated\_Sector\_Ct** value is greater than 128, this drive should be replaced.

**Table 9-3 RMA Case—Replace HDD Example**

ID#	ATTRIBUTE_NAME	FLAG	VALUE	WORST	THRESH	TYPE	UPDATED	RAW_VALUE
1	Raw_Read_Error_Rate	0x000f	072	063	044	Pre-fail	Always	59861501
3	Spin_Up_Time	0x0003	099	099	000	Pre-fail	Always	0
4	Start_Stop_Count	0x0032	100	100	020	Old_age	Always	12
<b>5</b>	<b>Reallocated_Sector_Ct</b>	<b>0x0033</b>	<b>099</b>	<b>099</b>	<b>036</b>	<b>Pre-fail</b>	<b>Always</b>	<b>130</b>
7	Seek_Error_Rate	0x000f	072	060	030	Pre-fail	Always	17169006
9	Power_On_Hours	0x0032	090	090	000	Old_age	Always	9010
10	Spin_Retry_Count	0x0013	100	100	097	Pre-fail	Always	0
12	Power_Cycle_Count	0x0032	100	037	020	Old_age	Always	12
184	Unknown_Attribute	0x0032	100	100	099	Old_age	Always	0
187	Reported_Uncorrect	0x0032	093	093	000	Old_age	Always	7
188	Unknown_Attribute	0x0032	100	100	000	Old_age	Always	0
189	High_Fly_Writes	0x003a	100	100	000	Old_age	Always	0
190	Airflow_Temperature_Cel	0x0022	071	069	045	Old_age	Always	29 (Lifetime Min/Max 28/29)
194	Temperature_Celsius	0x0022	029	040	000	Old_age	Always	29 (0 22 0 0)
195	Hardware_ECC_Recovered	0x001a	052	011	000	Old_age	Always	59861501
<b>197</b>	<b>Current_Pending_Sector</b>	<b>0x0012</b>	<b>100</b>	<b>100</b>	<b>000</b>	<b>Old_age</b>	<b>Always</b>	<b>1</b>

**Table 9-3 RMA Case—Replace HDD Example (continued)**

ID#	ATTRIBUTE_NAME	FLAG	VALUE	WORST	THRESH	TYPE	UPDATED	RAW_VALUE
198	Offline_Uncorrectable	0x0010	100	100	000	Old_age	Offline	1
199	UDMA_CRC_Error_Count	0x003e	200	200	000	Old_age	Always	0

Table 9-4 provides an example of the last part of the output of the **show disk SMART-info detail** command. The attributes that need to be reviewed to determine if the drive needs to be replaced or repaired are highlighted in bold. In this example, the Current\_Pending\_Sector and Offline\_Uncorrectable each have a value greater than one, so monitor these values over several days. The Latent Sector Error feature attempts to repair such errored sectors in a background process by deleting (evicting) corrupted content. If after several days of monitoring the values for Current\_Pending\_Sector and Offline\_Uncorrectable have not decreased, consider running the **disk repair** command.

**Table 9-4 Disk Repair Case—Repair HDD Example**

ID#	ATTRIBUTE_NAME	FLAG	VALUE	WORST	THRESH	TYPE	UPDATED	RAW_VALUE
1	Raw_Read_Error_Rate	0x000f	072	063	044	Pre-fail	Always	59861501
3	Spin_Up_Time	0x0003	099	099	000	Pre-fail	Always	0
4	Start_Stop_Count	0x0032	100	100	020	Old_age	Always	12
<b>5</b>	<b>Reallocated_Sector_Ct</b>	<b>0x0033</b>	<b>099</b>	<b>099</b>	<b>036</b>	<b>Pre-fail</b>	<b>Always</b>	<b>5</b>
7	Seek_Error_Rate	0x000f	072	060	030	Pre-fail	Always	17169006
9	Power_On_Hours	0x0032	090	090	000	Old_age	Always	9010
10	Spin_Retry_Count	0x0013	100	100	097	Pre-fail	Always	0
12	Power_Cycle_Count	0x0032	100	037	020	Old_age	Always	12
184	Unknown_Attribute	0x0032	100	100	099	Old_age	Always	0
187	Reported_Uncorrect	0x0032	093	093	000	Old_age	Always	<b>0</b>
188	Unknown_Attribute	0x0032	100	100	000	Old_age	Always	0
189	High_Fly_Writes	0x003a	100	100	000	Old_age	Always	0
190	Airflow_Temperature_Cel	0x0022	071	069	045	Old_age	Always	29 (Lifetime Min/Max 28/29)
194	Temperature_Celsius	0x0022	029	040	000	Old_age	Always	29 (0 22 0 0)
195	Hardware_ECC_Recovered	0x001a	052	011	000	Old_age	Always	59861501
<b>197</b>	<b>Current_Pending_Sector</b>	<b>0x0012</b>	<b>100</b>	<b>100</b>	<b>000</b>	<b>Old_age</b>	<b>Always</b>	<b>3</b>
<b>198</b>	<b>Offline_Uncorrectable</b>	<b>0x0010</b>	<b>100</b>	<b>100</b>	<b>000</b>	<b>Old_age</b>	<b>Offline</b>	<b>3</b>
199	UDMA_CRC_Error_Count	0x003e	200	200	000	Old_age	Always	0



**Note** The Latent Sector Error feature attempts to repair errored sectors in a background process by deleting (evicting) corrupted content. If after several days of monitoring the values for Current\_Pending\_Sector and Offline\_Uncorrectable have not decreased, consider running the **disk repair** command.

The **show disk SMART-info detail** command only reports sector errors that have been detected; there

may be more sectors in error adjacent to the reported bad sector. Repairing the drive also proactively repairs unreported sector errors. However, because repairing a drive is a time-consuming process, it may be easier to just replace the drive if a spare drive is available.

**Table 9-5** provides detailed description of the Attribute Names that could indicate disk problems primarily applicable to HDDs.

**Table 9-5 Attribute Names Descriptions—Disk Problem Indicators**

ID	Attribute Name	Description
5	Reallocated Sectors Count	<p>Count of reallocated sectors. When the hard drive finds a read/write/verification error, it marks that sector as "reallocated" and transfers data to a special reserved area (spare area). This process is also known as remapping, and reallocated sectors are called <i>remaps</i>. The raw value normally represents a count of the bad sectors that have been found and remapped; thus, the higher the attribute value, the more sectors the drive has had to reallocate. This allows a drive with bad sectors to continue operation; however, a drive that has had any reallocations at all is significantly more likely to fail in the near future. While primarily used as a metric of the life-expectancy of the drive, this number also affects performance. As the count of reallocated sectors increases, the read/write speed tends to worsen because the drive head is forced to seek to the reserved area whenever a remap is accessed. A workaround, which preserves drive speed at the expense of capacity, is to create a disk partition over the region that contains remaps and instruct the operating system to not use that partition.</p> <p>If the drive can repair the sector without remapping it, then the Reallocated Sectors Count is not incremented. If the drive must remap the sector, the Reallocated Sectors Count is incremented.</p>
197	Current Pending Sector Count	<p>Count of “unstable” sectors (waiting to be remapped, because of read errors). If an unstable sector is subsequently read successfully, this value is decreased and the sector is not remapped. Read errors on a sector do not cause a remap of the sector, because the sector might be readable later. Instead, the drive firmware remembers that the sector needs to be remapped, and remaps it the next time it is written.</p> <p>Running the <b>disk repair</b> command resolves these counts.</p>
198	Uncorrectable Sector Count or Offline Uncorrectable or Off-Line Scan Uncorrectable Sector Count	<p>The total count of uncorrectable errors when reading/writing a sector. A rise in the value of this attribute indicates defects of the disk surface, problems in the mechanical subsystem, or both.</p> <p>Running the <b>disk repair</b> command resolves these counts.</p>

#### Other Disk-Related show Commands

Additionally, the CDSM GUI and the CLI on the SEs display information about the disk-related alarms with the **show alarms** command, and information about the disk and sector related errors with the **show disks error-handling** command and the **show disks error-handling details** command. If sector alarms have occurred, enter the **show disk SMART-info details** command on the SE to determine the state of the drive and whether the drive needs to be replaced or potentially manually repaired using the **disk repair** command.

Following is an example of the **show alarms** command output:

Minor Alarms:

-----

Alarm ID	Module/Submodule	Instance
1 badsector	sysmon	disk01
2 badsector	sysmon	disk08

Following is an example of the **show disks error-handling** command output:

```
# show disks error-handling
disk05: Total bad sectors = 1, total errors = 2
disk10: Total bad sectors = 3, total errors = 9

Total failed disks = 0
```

Following is an example of the **show disks error-handling details** command;

```
# show disks error-handling details
disk05: Total bad sectors = 1, total errors = 2
    disk05: sector (LBA): 3000005      errors: 2

disk10: Total bad sectors = 3, total errors = 9
    disk10: sector (LBA): 16000      errors: 3
    disk10: sector (LBA): 170001     errors: 4
    disk10: sector (LBA): 180001     errors: 2

Total failed disks = 0
```

The **details** keyword displays the logical block address (LBA) for each bad sector along with the corresponding I/O error count.

## disk repair Command

This section describes the **disk repair** command.



### 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 takes approximately three hours to complete per disk. The **disk repair** command takes approximately 30 minutes on a solid-state drive (SSD).

Running the **disk repair** command erases all content on the drive. Never run the **disk repair** command on a “live” system.

### Overview

The **disk repair** command detects and repairs bad sectors across an entire drive on an SE, SR and CDSM, then reformats the drive. All data on the drive is lost, but the sectors are repaired and available for data storage again.

### Usage

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
```

The **sector** keyword is optional. If the **sector** keyword is omitted, the entire disk is repaired. If the **sector** keyword is specified along with the *sector\_address\_in\_decimal*, then only a small area of the disk is repaired (approximately 2 GB on either side of the sector address specified). The **sector** keyword should only be used if the disk has a single sector error; that is, if the output of the **show disk SMART-info details** command shows 1 unrecoverable pending sector in error; otherwise, omit the **sector** keyword to repair the entire disk drive.

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"

The command is limited to repairing one disk at a time. Supplying multiple disk names to the **disk repair** command is considered invalid input, and results in the command displaying the syntax information.

### Output

Following is an example of the output displayed when the **disk repair** command is running:

```
Repairing disk01 [140013/140013] (100%) rate: 51(MB/s) eta: 4(s)
Repaired LBA 286747000 (total: 1)
Repaired LBA 286747999 (total: 2)
Repairing disk01 [140014/140013] (100%) rate: 51(MB/s) eta: 4(s)
Recovery complete (2 sectors repaired)
Check syslog for more details
```

### Progress Indicator

The progress indicator is frequently updated to provide the user with up-to-date statistics and progress of the repair. Following is an example of the progress indicator:

```
Repairing disk01 [140013/140013] (100%) rate: 51(MB/s) eta: 4(s)
Repairing disk01 [140013/140013] (100%) rate: 51(MB/s) eta: 4(s)
```



**Note** Rate and ETA fields provide approximate estimates. The rate field does not indicate the top performance of the drive.

---

Performance of low-level utilities can vary as much as 30 percent across different VDS-IS releases.

### Repair Notice

Each time the **disk repair** command detects and repairs a sector, a simple message is displayed that describes the location of the repair as well as the cumulative total of repairs. Following is an example:

```
Repaired LBA 286747000 (total: 1)
```

### Syslog

To provide a history of the repair, the **disk repair** command logs basic test information (start / stop / failures) along with the address of every sector repaired.

```

repair-disk disk01: %SE-UNKNOWN-5-899999: Starting recovery
repair-disk disk01: %SE-UNKNOWN-5-899999: Repaired LBA 286747000 (total: 1)
repair-disk disk01: %SE-UNKNOWN-5-899999: Repaired LBA 286747999 (total: 2)
repair-disk disk01: %SE-UNKNOWN-5-899999: Recovery complete (2 sectors repaired)

```

## Removing and Replacing Disk Drives

In brief, the procedure for replacing a disk is simply to enter the **disk unuse** command, optionally 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. If when a new disk is added, the disk manager detects "degraded" or "bad" system volumes, the new disk is used to repair the system volumes. Thus, the disk manager always strives to have two disks allocated to the system volumes. If when a new disk is added, the system volumes are "normal" or "syncing," the new disk is added to the cdnfs volume.

For non-CDEs, the system disk cannot be easily replaced. If a system disk needs to be replaced on a non-CDE, it needs to have the VDS-IS software reinstalled by using the Recovery CD-ROM. For more information, see the "[Using the Cisco VDS-IS Software Recovery CD-ROM](#)" section on page 9-17.

The CDE250-2S6 and CDE25-2S3i have fixed bay mappings for internal drives. If the internal drives show as "degraded" or "bad" on these platforms and a new drive is inserted into one of the external slots, the disk manager allocates the disk as CDNFS, not SYSTEM. A failed internal drive requires that the CDE be replaced.

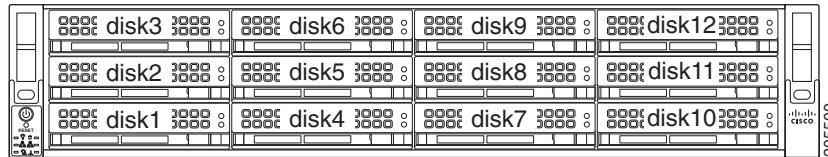


**Note** For the, CDE250-2S6, CDE250-2S8, CDE250-2S9, and CDE250-2S10, because the system disks are internal drives, if the system disk is "bad," the CDE should be replaced. However, it may be possible to repair the internal drive using the **disk repair** command, and let the system rebuild the SYSTEM RAID drives.

The disk numbering on the CDE250 starts on the left side at disk00, with the last disk being disk23.

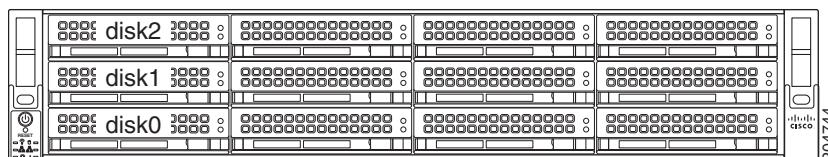
[Figure 9-2](#) shows the disk numbering on a CDE220.

**Figure 9-2** *Disk Numbering on a CDE220*



[Figure 9-3](#) shows the disk numbering on a CDE205.

**Figure 9-3** *Disk Numbering on a CDE205*



## Replacing a Disk

When replacing a disk, the new disk is recognized and for SYSTEM drives, the RAID is rebuilt. After inserting the new disk, enter the **disk policy apply** command to force the VDS-IS software to detect the new disk and rebuild the RAID. After replacing the disk, we recommend that you reboot the SE to ensure all VDS-IS software services are functioning correctly.

To replace a disk on a device, follow these steps:

- 
- Step 1** Offload the device. In the CDSM GUI, choose **Devices > Devices > Device Activation**, check the **Server Offload** check box, and click **Submit**.
  - Step 2** Enter the **show disk details** command to see if the drive is mounted. If the drive is mounted, enter the **disk unuse** command to fully unuse the drive. The **disk unuse** command safely shuts down the drive, guaranteeing all background drive activity is halted. This prevents accidental data loss when removing or power cycling the device.
  - Step 3** Remove the bad disk and insert the new disk.
  - Step 4** If the output for the **show disk details** command shows the drive bay as “bad,” enter the **disk mark diskname good** command to mark the drive bay good. For example, if you replaced disk 5 on a CDE220 (see [Figure 9-2](#)), you would enter the following command:  
`disk mark disk05 good`
  - Step 5** As a precaution, run the **disk erase diskXX** command to place the drive in the unformatted state and reboot the device.
  - Step 6** Enter the **disk policy apply** command to format and mount the drive, examine all disks and RAID volumes, and make any necessary changes. If the device was rebooted after the **disk erase** command, the **disk policy apply** command is started automatically at boot-up.

If new drives and system volumes are degraded or bad, the new drive is added as a SYSTEM/RAID volume; otherwise, the drive becomes a CDNFS drive.

Additionally, any detected unused drives are reused (mounted). If there are no new drives and everything is mounted, the command has no effect.
  - Step 7** Enter the **show disk details** command to see if the drive was added as a SYSTEM drive. If so, enter the **show disk raid** command to verify that the RAID volumes have been completely resynchronized.
  - Step 8** Return the device to online status. In the CDSM GUI, choose **Devices > Devices > Device Activation**, uncheck the **Server Offload** check box, and click **Submit**.
- 

The VDS-IS software marks the drive bay as good or bad, as opposed to the disk itself. Marking the bay helps avoid the scenario where a bad disk looks good during the next boot, which for disks is almost always the case. As such, simply placing a new disk into a bad bay does not automatically mark the bay good. Once more, if a bad disk is moved to a good bay, the system would not immediately recognize the disk as faulty.



**Note** Replacing a bad disk with a good disk from another CDE is not supported. If the disk is already in use on another CDE when it is removed and inserted into the current CDE, then the disk is used without reformatting, which creates problems.

The proper way to erase a disk after transplanting is as follows:

```
disk erase diskXX  
disk policy apply diskXX
```

**Note**

If you encounter an “unreadable sectors on the disk” condition, contact Cisco Technical Support for information on the **disk repair** command. For more information about the **disk repair** command, see the “[disk repair Command](#)” section on page 9-32



## APPENDIX

# A

## Troubleshooting

---

This appendix provides information on troubleshooting. The following topics are covered in this appendix:

- [Troubleshooting Service Router Configurations, page A-1](#)
- [Troubleshooting the Distribution Hierarchy, page A-2](#)
- [Troubleshooting Content Acquisition, page A-3](#)
- [Enabling the Kernel Debugger, page A-6](#)
- [Troubleshooting Web Engine Cache Status Codes, page A-7](#)

For more troubleshooting tools, see [Chapter 8, “Monitoring the Videoscape Distribution Suite, Internet Streamer.”](#)

## 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. Here are some areas to look at when troubleshooting:

- 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? See the [“Activating a Service Router” section on page 4-100](#) to activate a Service Router.
  - Is a default coverage zone set for a Service Engine, or is there a Videoscape Distribution Suite, Internet Streamer (VDS-IS) network-wide Coverage Zone file or a local Coverage Zone file set for the Service Router? See the [“Coverage Zone File Registration,” page 6-12](#) to set a Coverage Zone file. See the [“Configuring the Service Engine” 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.” See the [“Coverage Zone File” section on page 1-38](#) for information on coverage zones. See [Appendix C, “Creating Coverage Zone Files,”](#) for information on creating a Coverage Zone file.

## Troubleshooting the Distribution Hierarchy

- Is the serving Service Engine activated? See the “Activating a Service Engine” section on page 4-10 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? See the “Creating Delivery Service” section on page 5-16.
- Is the serving Service Engine alive? Use the **show statistics service-routing se** command to show the status of a Service Engine. See the “Using show and clear Commands” section on page 8-17.
- Content prefetched on a Service Engine
  - Is a Manifest file assigned to the Delivery Service associated with the serving Service Engine? See the “Working with Manifest Files” section on page B-2.
  - Is the Manifest file accessible from the CDSM? See the “Identifying Content Using a Manifest File” section on page 5-43.
  - Is there any syntax error in the Manifest file? See the “Manifest File Structure and Syntax” section on page B-19.
  - Is the requested content specified in the Manifest file? See the “Specifying a Single Content Item” section on page B-2.
  - If the requested content is streaming media, is the protocol engine enabled? See the “Application Control” section on page 4-34.

For general information, use the **show statistics service-router all** command.

# 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.

- 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:

```
cel# show distribution remote traceroute ?
forwarder-next-hop next forwarder along the path
unicast-sender     check status for unicast sender

cel# show distribution remote traceroute forwarder-next-hop ?
delivery-service-id Delivery-service-id of a Delivery Service

cel# 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

cel# 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 RootCE)
```

- 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:

```
sel# 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

sel# 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

sel# 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 the following commands from the Content Acquirer CLI:

- 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-CE-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

```

- 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

```

- 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
-----
```

**Troubleshooting Content Acquisition**

```
Acquired Single Items : 0 / 0
Acquired Crawl Items : 2237 / 2500 -- start-url=www.mtv.com//
```

- 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
```

- 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
```

- 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.
- 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:

```
SE# show distribution object-status
http://172.18.81.168/videos/SM-final%20Innebandy%202003.wmv
=====
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/19/19f6d5cec7266c33f419709dc28c
8d9b.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/19/19f6d5cec7266c33f419709dc28c
8d9b.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-k5bsm1o+y14jgiqsvwaohq/19/19f6d5cec7266c33f419709dc28c
8d9b.0.data.wmv

```

## ■ Enabling the Kernel Debugger

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.

- 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-g1fc4h-b9gywnf5rlnfweg/
            http-172.18.81.163-og5o2lu178nrhw1mctgtiq/
            172.18.81.163/
            file--xrnfxwifgu62jtiwtyixvg/
            172.18.81.168/
            http-172.18.81.168-k5bsmlo+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 VDS-IS 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, follow these steps:

- 
- Step 1** Choose **Devices > Devices > General Settings > Troubleshooting > Kernel Debugger**. The Kernel Debugger page is displayed.
- Step 2** To enable the kernel debugger, check the **Enable** check box, and click **Submit**.
- 

## Troubleshooting Web Engine Cache Status Codes

Generally speaking, a TCP\_MISS/504 status code can occur in a multi-tier system at two places:

- Between the downstream SE and the upstream SE
- Between the Content Acquirer and the Origin Server

Normally, the verification of a 504 status code is a bottom up procedure; that is, start from the edge SE and end at the Origin Server. Following is an example of the bottom-up checking procedure for a 504 status code in a three-tiered system:

1. If a 504 status code is observed on the edge SE, then the transaction logs on the middle SE should be checked to see what the status code is for that request.
2. If the status code on the middle SE is also 504, then check the transaction logs on the Content Acquirer to see what the status code of that request is:
  - a. If the status code on the Content Acquirer is also 504, it means the Origin Server is taking too much time to respond and the Content Acquirer timeout period expires. Check the Origin Server to see why it is not responding in a timely manner.
  - b. If the status code on the Content Acquirer is not 504 (for example, it is 200), it means the Origin Server is responding to the Content Acquirer quickly enough; however, the Content Acquirer somehow takes too much time to respond to the middle SE. If this is the case, investigate why the Content Acquirer is busy.
3. If the status code on the middle SE is not 504, similar to the Content Acquirer case mentioned above, it means the Content Acquirer is responding to the middle SE quickly enough (the transaction logs on the Content Acquirer should confirm this); however, the middle SE somehow take too much time to respond the edge SE. If this is the case, investigate why the middle SE is busy.

Basically, a 504 status code is normally caused by the upstream device taking too much time to respond to the downstream device. This troubleshooting section only covers the investigation of the upstream SEs. A 504 status code can occur on the upstream SE for the following reasons:

- Network-related issues between the downstream device and upstream device
- Issues inside the upstream SEs
- Configuration related issue

**Table A-1** provides more information about the scenarios where the 504 status code was observed, the tools used to investigate the scenarios, and the investigation results of each one.

**Table A-1 Scenarios of 504 Status Codes**

Scenario	Investigation Results
<b>Network Related Issue Between Downstream Device and Upstream Device</b>	
Tools used to investigate were the following: tcpdump, netstat, netmon, iostat, mpstat, and ping.	
<ul style="list-style-type: none"> <li>Three-tier system</li> <li>504 seen on the middle SE</li> <li>Content Acquirer had 200 hits for the same entry</li> </ul>	<ul style="list-style-type: none"> <li>Network interface cards throughput was under limit</li> <li>Disks were not overloaded</li> <li>Traffic had no problems for a long time, but at certain moments saw all dropped to 504s</li> <li>Output from the <b>tcpdump</b> command shows response packet never reached Content Acquirer to middle SE</li> <li>Checked reachability by running the <b>ping</b> command at the same time as when the 504 status code was seen. The ping request was getting dropped all of the sudden.</li> <li>System administrators confirmed that Content Acquirer was on a different switch, and that there might be some other load on that switch.</li> </ul>
<ul style="list-style-type: none"> <li>Two-tier system</li> <li>504 seen on the edge SE</li> <li>Content Acquirer had 200 hits for the same entry</li> </ul>	<ul style="list-style-type: none"> <li>Client to the edge SE has 40 GB network capacity, while edge SE to Content Acquirer has only 4 GB network capacity</li> <li>Client simulator puts out 2,000 Sim Users with 3Mbps traffic for peak (6 Gbps), stressing the 4-GB limit between edge SE and Content Acquirer</li> <li>Smooth traffic eventually balances itself out with lower Mbps, but some 504 status codes are seen between the Content Acquirer and middle SE, resulting in packet drops</li> <li>Output from the <b>netmon</b> command shows steady traffic increase followed by sudden drop</li> </ul>
<ul style="list-style-type: none"> <li>Two-tier system</li> <li>504 seen on the edge SE</li> <li>200 seen on the Content Acquirer for the same request</li> </ul>	<ul style="list-style-type: none"> <li>Client to edge SE has 2 GB throughput capacity, which was not exceeded in the tests</li> <li>Origin Server to Content Acquirer has 2 GB throughput capacity, which was not exceeded in the tests</li> <li>Disk is not a bottleneck on the Content Acquirer as verified by iostat</li> <li>CPU is not a bottleneck on the Content Acquirer as verified by mpstat</li> <li>Running netmon on both the edge SE and Content Acquirer reveals that all edge interfaces were used on edge SE; however, only one or two interfaces on the Content Acquirer were used</li> <li>Found that the Cisco Catalyst 3750 switch is used in the test bed, which only supports IP-based load balancing. SEs have interfaces bound to a particular port channel with one IP address so that only one interface on the switch is selected for the data transfer between the edge SE and Content Acquirer; therefore, the 1-GB interface can cause issue when traffic is over 1 GB</li> </ul>

**Table A-1 Scenarios of 504 Status Codes (continued)**

Scenario	Investigation Results
<b>Issues Inside the Upstream SEs</b>	
Tools used to investigate were the following: mpstat and iostat.	
<ul style="list-style-type: none"> <li>• Three-tier system</li> <li>• 504 seen on edge and middle SEs</li> <li>• Content Acquirer had 20 million content objects cached</li> </ul>	<ul style="list-style-type: none"> <li>• Output from the <b>isostat</b> command for certain disks on the Content Acquirer was sometimes showing individual request serving time in range of seconds</li> <li>• Output from the <b>iostat</b> command for particular disk showed the usage was 100 percent, and the time interval between I/O requests issued to the device, and being served from the device, was very high</li> <li>• Output from the <b>show alarms history detail</b> command showed CPU and diskthreshold alarm raised</li> </ul>
<ul style="list-style-type: none"> <li>• Three-tier system</li> <li>• 504 seen on edge and middle SEs</li> <li>• Reload Content Acquirer</li> </ul>	<ul style="list-style-type: none"> <li>• Only CDE250-2M0 shows this behavior and only during reload</li> <li>• After investigating components (network and disk), questioned lookup queue response</li> <li>• Output from the <b>show statistics web-engine detail</b> command showed large outstanding lookup requests on the Content Acquirer</li> <li>• Inserted an instrument into lookup queue size check, which showed queue size for lookup increasing to 200–300 range during reload, while in normal operation the queue was always in the single digits.</li> <li>• Observed CPU cycle during reload, it showed that even though there were some free cycles, it was not enough to finish sudden intake of request lookup</li> <li>• Content Manager scans during the beginning of a reload, and because the CDE250-2M0 has different disk types, it takes up a lot of the CPU, leaving a large lookup queue</li> </ul>
<ul style="list-style-type: none"> <li>• Two-tier system</li> <li>• 504 seen on edge SE</li> <li>• 504 and NONE/000 seen on Content Acquirer</li> <li>• 20 million content objects cached on both edge SE and Content Acquirer</li> <li>• 800 transactions per second</li> <li>• Small file (240 KB) all unique cache miss</li> <li>• CDE250-2G2</li> <li>• No core dump files</li> <li>• Long running time (92 hours)</li> </ul>	<ul style="list-style-type: none"> <li>• Output from the <b>show alarms history detail</b> command on the edge SE showed servicedead, memory, session, CPU, disk, and cal_diskwrite_exceed alarms raised</li> <li>• Output from the <b>show alarms history detail</b> command on the Content Acquirer showed CPU, disk, and cal_diskwrite_exceed alarms raised</li> <li>• CDE250-2G2 capacity exceeded</li> </ul>

**Table A-1 Scenarios of 504 Status Codes (continued)**

Scenario	Investigation Results
<b>Configuration Related Issue</b>	
(Only applicable if trace-level logging is enabled)	
<ul style="list-style-type: none"> <li>• Three-tier system</li> <li>• 504 seen on edge and middle SE</li> </ul>	<ul style="list-style-type: none"> <li>• Trace-level errorlog was enabled on all SEs</li> <li>• Top showed that unified_errlogd, the process handling errorlog writing, used a lot of the CPU, when CPU usage hit 100 percent, 504 started happening</li> <li>• Traces in the system can be enabled for debugging purposes; however, if they are enabled, they cause a very large number of disk I/O accesses, which causes the Content Acquirer to take a long time to respond</li> </ul>



## Creating Manifest Files

---

This appendix describes the process for creating Manifest files used to acquire and distribute content within the VDS-IS network. This appendix includes the following topics:

- [Introduction, page B-1](#)
- [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-47](#)

For information about using a Manifest file in a Delivery Service, see the “[Identifying Content Using a Manifest File](#)” section on page [5-43](#).

## Introduction

The VDS-IS 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 inter-operate with the VDS-IS by using this Manifest file interface. Each Delivery Service in the VDS-IS 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 the following:

- 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 VDS-IS 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.

## Working with Manifest Files

This section provides Manifest file samples for carrying out specific tasks. 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

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.

The following example provides an example of a Manifest file that specifies single content items:

```
<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, you 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 <server><host> 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, ... = Acquire the starting URL and its referred files to the depth specified. -1 = Infinite or no depth restriction.  If the depth is not specified, the default is used. The default is 20.  <b>Note</b> 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.

**Table B-1 Website or FTP Server Crawl Job Attributes (continued)**

Attribute	Description
<i>prefix</i>	<p>(Optional) Combines the hostname from the &lt;server&gt; 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:</p> <pre data-bbox="584 424 1481 475">&lt;server name="xx"&gt; &lt;host name="www.cisco.com" proto="https" port=433/&gt; &lt;/server&gt;</pre> <p>with the following &lt;crawler&gt; tag:</p> <pre data-bbox="584 551 878 576">prefix="marketing/eng/"</pre> <p>The full prefix is “<a href="https://www.cisco.com:433/marketing/eng/">https://www.cisco.com:433/marketing/eng/</a>.” 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.</p> <p>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 “<a href="https://www.cisco.com:433">https://www.cisco.com:433</a>.”</p>
<i>accept</i>	<p>(Optional) Uses a regular expression to define acceptable URLs to crawl, in addition to having acceptable URLs match a prefix. For example, accept=“stock” means that only URLs that meet two conditions are crawled: the URL matches the prefix and also contains the regular expression string “stock.”</p>
<i>reject</i>	<p>(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.</p>
<i>max-number</i>	<p>(Optional) Specifies the maximum number of crawl job objects that can be acquired.</p>
<i>maxTotalSizeInMB</i> <i>maxTotalSizeInKB</i> <i>maxTotalSizeInB</i>	<p>(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).</p>
	<p><b>Note</b> 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.</p> <p>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.</p>
<i>externalPrefixes</i>	<p>(Optional) Specifies additional prefixes for crawl jobs to crawl multiple protocols or multiple websites. Prefixes are separated with a bar ( ).</p>
<i>externalServers</i>	<p>(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 &lt;host&gt; tag with the proper authentication information.</p>

**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.

The following is an example of a 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 the following example:

```
<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 the following example, only URLs that match “http://linux-1.cisco.com/icons” are acquired.

```
<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.”

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*=“2002-06-28 18:35:21” means the content acquisition job can only start on June 28, 2002 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, 2001 at 8:45 a.m.

```

<crawler
      start-url="index.html"
      depth="2"
      prefetch="2001-11-09 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 the following example:

```
<?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. In the following example, 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.

```
<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](#) lists and 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 VDS-IS 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 VDS-IS software supports playservers that play back the following prefetched content types on the VDS-IS network: HTTP, HTTPS, RTSP, and RTMP (Movie Streamer, Windows Media, Flash Media Streaming).

The VDS-IS 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 though the <playServerTable> tag, use MIME-type extension names to configure which playserver can play the particular prefetched content, as shown in the following example:

```
<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 VDS-IS 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 VDS-IS software temporarily stops serving the content. If the serving stop time is omitted, the VDS-IS software serves the content to the Service Engine until the content is removed by modifying the Manifest file or renaming the Delivery Service.

**Table B-3** Attributes for Content Serving (continued)

Attribute	Description
<i>ignoreQueryString</i>	<p>Playback attribute that can be used with the &lt;options&gt;, &lt;item-group&gt;, &lt;item&gt;, and &lt;crawler&gt; tags. If <i>ignoreQueryString</i> is set to true, then the VDS-IS 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.</p> <p>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 <i>ignoreQueryString</i> attribute is set to false, then the VDS-IS software does not use prefetched content from the request URL http://web-server/foo.</p> <p>However, if the <i>ignoreQueryString</i> attribute is set to true, then the VDS-IS software treats the request URL http://www-server/foo?id=xxx the same as http://www-server/foo and returns prefetched content.</p>
<i>wmtRequireAuth</i>	<p>(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.</p> <p><b>Note</b> 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.</p>

## 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*

In the Manifest file, the time string conforms 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, 2002 at 09:09:09 Pacific daylight saving time:

```
<options timeZone="PDT" />
```

```
<item src="index.html" prefetch="2002-09-05 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 pertains to checking the Manifest file; it does not pertain to checking 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 VDS-IS network. If you do not specify a time when you set the *expires* attribute, content is stored in the VDS-IS 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, 2003 at 2:00 p.m.

```
expires="2003-06-12 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 the following example. The live stream for the wmt-live content type is url=rtsp://www.company-web-site.org/tmp/ceo-talk.

```
<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.



**Note** Existing live content is deleted and replaced with the content specified in the Manifest file under the following conditions:

- You create two delivery services that use the same content origin server in the following way:
  1. Create a live streaming Delivery Service by using the CDSM GUI.
  2. Use a Manifest file to set up live streaming on a prefetch/caching Delivery Service by using the *type* attribute with wmt-live as the value and wmt-live as the *src*.
- You assign an SE to the prefetch/caching Delivery Service with the live Manifest file assigned, the existing live content is overwritten with the content specified in the Manifest file if the program name is the same (in this example, wmt-live).

This is because the content is the latest assigned, whichever was assigned last, whether it was by the prefetch/caching Delivery Service or the live streaming Delivery Service.

## Specifying Hybrid Ingest Content

For hybrid ingested content, the content is not prefetched into the VDS-IS 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.

Following is an example of a Manifest file for 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="2007-01-12 14:00:00 PST"
      serveStopTime="2007-04-12 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 VDS-IS 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 VDS-IS network.

## Running the Manifest Validator Utility

To access the Manifest Validator, follow these steps:

- 
- Step 1** Choose Services > Service Definition > Delivery Services > Tools > Manifest Validator.



**Note** You must first create a new Delivery Service or edit an existing Delivery Service before you can access the 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.

## Valid Manifest File Example

The following text 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 reported 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
```

**Manifest Validator Utility**

```

        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 VDS-IS network
- **INCORRECT**—Contains syntax errors and is unsuitable for deployment on your VDS-IS network

## 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 VDS-IS network.

## Manifest File Structure and Syntax

The VDS-IS Manifest file provides powerful features for representing and manipulating VDS-IS network data that can be easily edited using any simple text editor.

**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/>	<i>name</i> <sup>1</sup>	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	<i>name</i>	(Optional, but must have either <contentType> or <extension> tag.) Names the MIME-type content mapped to a playserver.
extension	None	<i>name</i>	(Optional, but must have either <contentType> or <extension> tag.) Names the file extension that is mapped to a playserver.

**Table B-4** Manifest File Tag Summary (continued)

Tag Name	Subelements	Attributes	Description	
options	<schedule/> <repeat/>	enableCookies expires failRetryInterval ignoreOriginPort ignoreQueryString	<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/>	<b>name</b>	Defines <i>only</i> one host from which content is to be retrieved.	
host	None	<b>name</b>  disableBasicAuth noProxy ntlmUserDomain password port proto	<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
proxyServer	None	<b>serverName</b>  disableBasicAuth ntlmUserDomain password	<i>port</i> <i>user</i> <i>uuencoded</i>	Specifies proxy server information.
item	<contains/> <schedule/> <repeat/>	<b>src</b>  authCookie cdn-url disableBasicAuth enableCookies expires failRetryInterval host ignoreOriginPort ignoreQueryString noProxy ntlmUserDomain password playServer port	<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.

**Table B-4** Manifest File Tag Summary (continued)

Tag Name	Subelements	Attributes	Description	
crawler	<matchRule/> <schedule><repeat>	<i>start-url</i> <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>	password playServer port prefetch prefix priority proto proxyServer reject reportBrokenLinks serveStartTime serveStopTime server srcPrefix sslAuthType ttl type user userDomainName uuencoded wmRequireAuth	Supports crawling of a website or FTP server.
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 VDS-IS network.
contains	None	<i>cdn-url</i>	(Optional) Identifies content objects that are embedded within the content item currently being described.	

## Manifest File Structure and Syntax

- Attributes that are required for a tag are shown in ***boldface italic*** font.

**Table B-5      Manifest File Nested Tag Relationships**

<CdnManifest>				
	<playServerTable> <playServer>			
		<contentType /> <extension />		
			</playServerTable> </playServer>	
	<options>			
		Manifest file shared attributes		
			</options>	
	<server>			
		<host/>		
			</server>	
	<item>			
		<contains />		
			</item>	
	<crawler>			
		<matchRule/>		
			</crawler>	
	<item-group>			
		<contains />		
			</item-group>	
				</CdnManifest>

## 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 VDS-IS 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.



**Note** The `<contentType />` *name* value cannot exceed 32 characters.

### 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.



#### Note

---

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-29](#) 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-29](#) 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-29 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 VDS-IS 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 VDS-IS 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 VDS-IS 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.



**Note** Existing live content is deleted and replaced with the content specified in the Manifest file under the following conditions:

- You create two delivery services that use the same content origin server in the following way:
  1. Create a live streaming Delivery Service by using the CDSM GUI.
  2. Use a Manifest file to set up live streaming on a prefetch/caching Delivery Service by using the *type* attribute with *wmt-live* as the value and *wmt-live* as the *src*.
- You assign an SE to the prefetch/caching Delivery Service with the live Manifest file assigned, the existing live content is overwritten with the content specified in the Manifest file if the program name is the same (in this example, *wmt-live*).

This is because the content is the latest assigned, whichever was assigned last, whether it was by the prefetch/caching Delivery Service or the live streaming Delivery Service.

- *playServer*

The *playServer* attribute is optional and names the server used to play back the content. Valid playservers 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 playserver or multiple playservers separated by commas. If a value for this attribute is not specified, the *<PlayServerTable>* tag in the Manifest file is used to generate the playserver 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, 2002 at 09:09:09 Pacific daylight saving time.

```
<options timeZone="PDT" />
<item src="index.html" prefetch="2002-09-05 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 VDS-IS 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.



**Note** Revalidation is enabled by default for the Web Engine.

<b><i>ttl</i> Attribute Value</b>	<b>Action</b>
<i>ttl</i> > 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 <b>Refetch</b> button.
<i>ttl</i> = 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 <b>Refetch</b> button.
<i>ttl</i> < 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 <b>Refetch</b> button.

- *serveStartTime*

The *serveStartTime* attribute is optional and designates a time in yyyy-mm-dd hh:mm:ss format when the VDS-IS 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 VDS-IS software temporarily stops serving the content. If the time to stop serving is omitted, the VDS-IS 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 VDS-IS 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 VDS-IS 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 VDS-IS 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 VDS-IS 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 ingest depends on the *ignoreQueryString* value and the protocol engine serving the content.

If Windows Media Streaming 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, Windows Media Streaming 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="2003-09-11 11:11:11 PST" end="2004-09-11 11:11:21
PST" />
            <repeat time="21:02:35" start="2003-09-11 11:11:11 PST" end="2004-09-11
11:11:21 PST"/>
            <repeat time="21:02:35" end="2004-09-11 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-29.)

- *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, ... = 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-6 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-6 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 VDS-IS 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 VDS-IS 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-29](#) 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-29 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*

## Manifest File Structure and Syntax

- *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 VDS-IS network URL using the following rules:

- If the *cdn-url* attribute is present in the `<item>` tag, the relative VDS-IS 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 VDS-IS 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 VDS-IS network URL is the *cdnPrefix* attribute plus the relative source URL.
- To generate a relative VDS-IS network URL, remove the matched prefix from the relative source URL and replace it with the *cdnPrefix* attribute.

The relative VDS-IS 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 VDS-IS 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-group>`
- `<item></item>`
- `<schedule><repeat>`

(See the “item” section on page B-29 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.



#### Note

The matchRule element is not supported for FTP; it is only supported for HTTP.

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 VDS-IS 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-47](#).)

- *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-47](#).)



**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="2000-05-05 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, 2003, 10:30 p.m., use the absolute time format, as shown in the following example:

```
<match time-after="2003-01-30 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 VDS-IS 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 VDS-IS software does not serve this item unless every contained item is present.

### Attributes

The *cdn-url* attribute is required and is the relative VDS-IS network URL of one of the embedded contents.

### Subelements

None

**Example**

```
<item src="house/img08.jspb" cdn-url="img08.jpg" />
<item src="house/img09.jspb" 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

In the case of the Manifest file, 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.

The XML Schema file describes and dictates the content of the XML file. The CdnManifest.xsd file contains the XML schema. To view or download a copy of the CdnManifest.xsd file, see the “[Viewing or Downloading XML Schema Files](#)” section on page 6-24.

## PlayServerTable XML Schema

The following XML code defines the PlayServerTable schema (playServerTable.xsd) for the CdnManifest.xsd:

```
<?xml version="1.0"?>
<xss:schema xmlns:xss="http://www.w3.org/2001/XMLSchema">
<xss:element name="playServerTable">
    <xss:complexType>
        <xss:sequence>
            <xss:element ref="playServer" minOccurs="1" maxOccurs="unbounded" />
        </xss:sequence>
    </xss:complexType>
</xss:element>
<xss:element name="playServer">
    <xss:complexType>
        <xss:choice minOccurs="1" maxOccurs="unbounded">
            <xss:element ref="contentType"/>
            <xss:element ref="extension"/>
        </xss:choice>
        <xss:attribute name="name" use="required">
            <xss:simpleType>
                <xss:restriction base="xs:string">
                    <xss:enumeration values="wmt"/>
                    <xss:enumeration values="http"/>
                    <xss:enumeration values="qtss"/>
                </xss:restriction>
            </xss:simpleType>
        </xss:attribute>
    </xss:complexType>
</xss:element>
<xss:element name="contentType">
    <xss:complexType>
        <xss:attribute name="name" type="xs:string" use="required"/>
    </xss:complexType>
</xss:element>
<xss:element name="extension">
    <xss:complexType>
        <xss:attribute name="name" type="xs:string" use="required"/>
    </xss: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/2001/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). [Table B-6](#) through [Table B-21](#) list the time zones supported by the Manifest file. The format for writing the time zone is:

*<zonename>:[+|-:]hh:mm per line*

In this format, *<zonename>* 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 “+.”

**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
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	—

**Table B-7 Africa GMT Offsets**

<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>
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	—

**Table B-8 America GMT Offsets**

<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>
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

**Table B-8 America GMT Offsets (continued)**

<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>
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
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/Montevideo:-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

**Table B-9 Antarctica/Arctic GMT Offsets**

<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>
Antarctica/Casey:+08:00	Antarctica/McMurdo:+12:00	Antarctica/Vostok:+06:00
Antarctica/Davis:+07:00	Antarctica/Palmer:-04:00	Arctic/Longyearbyen:+01:00

**Table B-9 Antarctica/Arctic GMT Offsets (continued)**

<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>
Antarctica/DtDUrville:+10:00	Antarctica/South_Pole:+12:00	—
Antarctica/Mawson:+06:00	Antarctica/Syowa:+03:00	—

**Table B-10 Asia GMT Offsets**

<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>
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
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/Urumsqi:+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	—

**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	—

**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
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

**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	—	—

**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-Saskatchewan:-06:00	Canada/Pacific:-08:00	Chile/EasterIsland:-06:00
Canada/Eastern:-05:00	Canada/Saskatchewan:-06:00	Cuba:-05:00

**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

**Table B-15 Egypt/Eire/Europe GMT Offsets (continued)**

<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>
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
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

**Table B-16 Hong Kong/Iceland/India/Iran/Israel GMT Offsets**

<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>
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

**Table B-17 Jamaica/Japan/Kwajalein/Libya GMT Offsets**

<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>
Jamaica:-05:00	Kwajalein:+12:00	Libya:+02:00
Japan:+09:00	—	—

**Table B-18 Mexico/Mideast GMT Offsets**

<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>	<b>Time Zone: GMT Offset</b>
Mexico/BajaNorte:-08:00	Mexico/General:-06:00	Mideast/Riyadh88:+03:07
Mexico/BajaSur:-07:00	Mideast/Riyadh87:+03:07	Mideast/Riyadh89:+03:07

**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/Fakaofo:-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

**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	—

**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	—



## Creating Coverage Zone Files

This appendix describes the Coverage Zone file and provides several Coverage Zone file examples.

### Introduction

A *Coverage Zone file* is an XML file used to specify a user-defined coverage zone. The Coverage Zone file supports different tags to support different types of proximity configurations.

- Network and subnet—Specify the IP address range
- Geographical location—Specify the longitude and latitude of the data center

In addition to the coverage zone information, two optional elements are created for documentation purposes: a revision value to specify the version of the Coverage Zone file and a customer name.

For information about importing or uploading a Coverage Zone file, see the “[Coverage Zone File Registration](#),” page 6-12.

For more information about Coverage Zone files, see the “[Coverage Zone File](#)” section on page 1-38.

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 VDS-IS network.

The XML Schema file describes and dictates the content of the XML file. The CdsCoverageZone.xsd file contains the XML schema. To view or download a copy of the CdsCoverageZone.xsd, see the “[Viewing or Downloading XML Schema Files](#)” section on page 6-24.



**Note**

When DNS-based redirection is enabled, the Coverage Zone file needs to have entries with respect to the IP address of the DNS proxies instead of the client IP address.

[Table C-1](#) defines the Coverage Zone file elements.

**Table C-1** *Coverage Zone File Elements*

Tag	Element	Value	Description
location	latitude	float	Value indicating the geographical coordinate (latitude) of the data center.
	longitude	float	Value indicating the geographical coordinate (longitude) of the data center.

**Table C-1** Coverage Zone File Elements (continued)

Tag	Element	Value	Description
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 VDS-IS release.
	customerName	customer name	Not used in this VDS-IS release.
	coverageZone	—	This can have one or more coverage zones.



**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.

## Zero-IP Based Configuration

The zero-ip based configuration is a catch-all condition for routing. It can be used in combination with proximity-based routing and location-based routing. If an SE cannot be found through location-based routing or proximity-based routing, the zero-ip based configuration is taken into account for selecting an SE.

The zero-ip based configuration 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-CDE220-1</SE>
    <metric>5</metric>
</coverageZone>
<coverageZone>
    <network>3.1.13.10/32</network>
    <SE>U8-CDE220-2</SE>
    <metric>5</metric>
</coverageZone>
<coverageZone>
    <network>0.0.0.0/0</network>
    <SE>U8-CDE220-3</SE>
    <metric>20</metric>
</coverageZone>
</CDNNetwork>
```

## Invalid IPv4 Addresses in Coverage Zone File

The following IPv4 addresses are considered invalid in the Coverage Zone file:

- Limited broadcast address (255.255.255.255)
- Class A (0.x.x.x)—These addresses are reserved.



**Note** The exception is 0.0.0.0/0, which is used for zero-IP based configuration.

- Class A (127.x.x.x)—These addresses are reserved. They are used as internal host loopback addresses, internal host loopback.
- Class B (191.255.x.x)—These addresses are reserved.
- Class C (223.255.255.x)—These addresses are reserved.
- Class D (224.x.x.x - 239.x.x.x)—Entire class is reserved for multicast addresses (the low order 24 bits represent the multicast group ID).
- Class E (240.x.x.x - 255.x.x.x)—Entire class is reserved for future use.

In addition, the following broadcast IPv4 addresses are not valid, and are not likely to be used in the Coverage Zone file:

- Class A (y.255.255.255, y = 1 to 127)—Directed broadcast to specified network.
- Class B (y.x.255.255, y = 128 to 191)—Directed broadcast to specified network.
- Class C (y.x.x.255, y = 192 to 223)—Directed broadcast to specified network.

## Coverage Zone File Example

The following sections show different Coverage Zone file examples in the following scenarios:

- [Scenario 1: Coverage Zone with Client Network Only](#)
- [Scenario 2: Coverage Zone with Geographical Location of the Datacenter Only](#)
- [Scenario 3: Coverage Zone with Client Network and Geographical Location of the Datacenter](#)
- [Scenario 4: Coverage Zone for Same Client Network with Different Weighted SEs](#)
- [Scenario 5: Coverage Zone with Restricted List of SEs Used for Proximity-Based Routing](#)
- [Scenario 6: Coverage Zone for IPv6 Client Networks](#)

For a proximity-based routing include list, the <coverageZone> tag just includes the <SE> and <metric> elements, as follows:

```
<!-- For proximity based routing include list -->
<coverageZone>
  <SE>W13-CDE205-1</SE>
  <SE>W13-CDE205-2</SE>
  <metric>10</metric>
</coverageZone>
```

**Coverage Zone File Example****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>CDE-200-SE1</SE>
        <SE>CDE-200-SE2</SE>
        <metric>10</metric>
    </coverageZone>
<!-- Chicago Datacenter -->
    <coverageZone>
        <network>192.1.3.0/24</network>
        <SE>CDE-200-SE3</SE>
        <SE>CDE-200-SE4</SE>
        <metric>10</metric>
    </coverageZone>
<!-- New York Datacenter -->
    <coverageZone>
        <network>192.1.4.0/24</network>
        <SE>CDE-200-SE5</SE>
        <SE>CDE-200-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>CDE-200-SE1</SE>
        <SE>CDE-200-SE2</SE>
        <metric>10</metric>
    </coverageZone>
<!-- Chicago Datacenter -->
    <coverageZone>
        <location>
            <latitude>42</latitude>
            <longitude>-88</longitude>
        </location>
        <SE>CDE-200-SE3</SE>
        <SE>CDE-200-SE4</SE>
        <metric>10</metric>
    </coverageZone>
<!-- New York Datacenter -->
    <coverageZone>
        <location>
            <latitude>41</latitude>
```

```

        <longitude>-74</longitude>
    </location>
<SE>CDE-200-SE5</SE>
<SE>CDE-200-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>CDE-200-SE1</SE>
        <SE>CDE-200-SE2</SE>
        <metric>10</metric>
    </coverageZone>
<!-- Chicago Datacenter -->
    <coverageZone>
        <location>
            <latitude>41</latitude>
            <longitude>-74</longitude>
        </location>
        <SE>CDE-200-SE3</SE>
        <SE>CDE-200-SE4</SE>
        <metric>10</metric>
    </coverageZone>
<!-- New York Datacenter -->
    <coverageZone>
        <network>192.1.4.0/24</network>
        <SE>CDE-200-SE5</SE>
        <SE>CDE-200-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>

```

**Coverage Zone File Example**

```

<SE> dmz2-is </SE>
<metric> 20 </metric>
</coverageZone>
</CDNNetwork>
```

## Scenario 5: Coverage Zone with Restricted List of SEs Used for Proximity-Based Routing

```

<?xml version="1.0" ?>
<!-- Coverage Zone data in XML -->
<CDNNetwork>
    <revision>1.0</revision>
    <customerName>Cisco Systems</customerName>

    <!-- Coverage Zone for static routes -->
    <coverageZone>
        <network> 192.0.2.0/24 </network>
        <SE> philly1 </SE>
        <SE> philly2 </SE>
        <metric> 10 </metric>
    </coverageZone>

    <!-- For proximity-based routing include list -->
    <coverageZone>
        <SE> philly1 </SE>
        <SE> philly2 </SE>
        <SE> boston1 </SE>
        <SE> boston2 </SE>
        <SE> anywhere1 </SE>
        <SE> anywhere2 </SE>
        <metric>10</metric>
    </coverageZone>
    <!-- For location-based routing -->
    <coverageZone>
        <location>
            <latitude>40</latitude>
        </location>
        <SE> philly1 </SE>
        <SE> philly2 </SE>
        <metric>10</metric>
    </coverageZone>

    <coverageZone>
        <location>
            <latitude>42</latitude>
            <longitude>71</longitude>
        </location>
        <SE> boston1</SE>
        <SE> boston2 </SE>
        <metric>10</metric>
    </coverageZone>

    <!-- all zeros -->
    <coverageZone>
        <network> 0.0.0.0/0 </network>
        <SE> anywhere1 </SE>
        <SE> anywhere2 </SE>
        <metric> 10 </metric>
    </coverageZone>
</CDNNetwork>
```

## Scenario 6: Coverage Zone for IPv6 Client Networks

```
<?xml version="1.0"?>
<CDNNetwork>
    <revision>1.0</revision>
    <customerName>Cisco Systems</customerName>
        <coverageZone>
            <network>2001:0DB8:0000:0001::/64</network>
            <SE>SE-1</SE>
            <metric>10 </metric>
        </coverageZone>
        <coverageZone>
            <network>::/0</network>
            <SE>SE-2</SE>
            <metric> 30 </metric>
        </coverageZone>
    </CDNNetwork>
```

■ Coverage Zone File Example



## Creating Geo/IP Files

This appendix describes the Geo/IP configuration file used by a Delivery Service to specify the geographic regions in which client requests are either allowed or denied.

### Introduction

The Geo/IP file is an XML file used to specify the geographic regions that are allowed or denied access to a Delivery Service, as well as the IP network that is allowed or denied access.

In addition to the allowed and denied geographical and network information, two optional elements are created for documentation purposes: a revision value to specify the version of the file and a customer name.

The Geo/IP files can be created using any ASCII text-editing tool. For information about uploading or importing a Geo/IP file, see the [“Authorization Plugins” section on page 5-27](#).

The XML Schema file describes and dictates the content of the XML file. The CDSAuthorization.xsd file contains the XML schema. To view or download a copy of the CDSAuthorization.xsd, see the [“Viewing or Downloading XML Schema Files” section on page 6-24](#).

Table D-1 defines the Geo/IP file elements.

**Table D-1** *Geo/IP 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) for IPv4 addresses. Both IPv4 and IPv6 addresses are supported.
	Geo		Describes the geographic region by country, state, city, Netspeed, connection_type, line_speed, asn, carrier, anonymizer_status, and generic attribute.

**Table D-1** Geo/IP 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, city, Netspeed, connection_type, line_speed, asn, carrier, anonymizer_status, and generic attribute.
Order	—	Allow, Deny	The order in which to apply the allow and deny rules. One of the following: <ul style="list-style-type: none"> <li>• Allow</li> <li>• Deny</li> <li>• Allow, Deny</li> <li>• Deny, Allow</li> </ul>
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.
	Netspeed	netspeed	Specifies the traffic in the specified network device.
	Connection_type	connection type	Specifies the connection type.
	Line_speed	line speed	Specifies the speed of the connection. The possible values are: <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> </ul>
	asn		Specifies the Autonomous System Number (ASN), that is corresponding to the senders IP address as retrieved from geo server/local geo cache. ASN value provided is a 32 bit integer.
	carrier		The carrier field provides the name of the organization responsible for the traffic carried on a particular network or set of networks designated as Autonomous System (AS).
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.

**Note**

For the Geo element, the country, state, and city names all must match what is used by the Geo-Location server. The names are case sensitive. If the country matches but the state and city names do not match, the request is denied. You can specify just the country, or the country and state, or the country, state, and city.

If the Geo element is defined, the Geo-Location servers are down or are not configured, and the client information is not found in the SE cache, a request denied message is returned to the client. The type of message that is returned depends on the protocol engine (for example, the Flash Media Streaming engine sends “Denied by auth server”). However, the client receives the same denied message from the protocol engine whether the client is denied based on the Authorization Service configuration, or based on the Geo-Location servers being down and the client information not being available in the SE cache.

Starting from Release 3.3, the Geo-Location servers support both IPv6 and IPv4 client configuration; therefore, geographic location authorization of client requests are supported for both IPv4 addresses and IPv6 addresses.

For more information on the Geo-Location server, see the “Geo-Location Servers” section on [page 4-107](#).

## Processing Order

When Geo/IP and Service Rules are configured, each client request goes through the following processing order:

1. SE bypass (this is used for multi-tiered SEs), no configuration is required
2. Service rules
3. Geo/IP Network element
4. Geo/IP Geo element

## Service Rule Config File

If the Service Rule file exists for the Delivery Service, it is processed before the Geo/IP file. If after going through the Service Rule conditions the client request is allowed, and there is a Geo/IP file associated with the Delivery Service, the client request goes through all the conditions defined in the Geo/IP file before the request is finally allowed.

# Understanding the Allow and Deny Conditions

The Geo/IP file allows client requests based on the Pattern element defined and either the Network element defined or Geo element defined, or both the Network and Geo elements defined.

**Note**

At least one Pattern element is required for the Allow tag and at least one Pattern element is required for the Deny tag.

At least one Network element or Geo element is required for the Allow tag and at least one Network element or Geo element is required for the Deny tag.

## Allow Conditions

Each element that is defined in the Allow tag (Pattern, Network, and Geo) must be matched for the client request to be allowed.

If only the Network element is defined for the Allow tag (no Geo element is defined), then the client request must only match the Network element for the request to be allowed. If only the Geo element tag is defined (no Network element is defined), then the client request must only match the Geo element for the request to be allowed.

If both the Network element and the Geo element are defined for the Allow tag, the client request must match both the Network and Geo element for the client request to be allowed.

If the Allow tag has multiple Network and Geo elements, at least one Network element must be matched and at least one Geo element must be matched in order for the client request to be allowed.

## Deny Conditions

At least one of the elements that is defined in the Deny tag (Pattern, Network, and Geo) must be matched for the client request to be denied.

If both the Network element and the Geo element are defined for the Deny tag, the client request must only match one of the conditions (either Network or Geo), for the client request to be denied.

If the Deny tag has multiple Network and Geo elements, only one condition must be matched (either Network or Geo) for the client request to be denied.

## Order Tag

The Order tag defines the order in which to apply the Allow and Deny tags. The Order tag can have the following settings:

- [Allow, Deny](#)
- [Deny, Allow](#)
- [Allow](#)
- [Deny](#)

### **Allow, Deny**

If the Order tag is set to <Allow, Deny>, and both the Network element and the Geo element are defined for both the Allow tag and the Deny tag, first the request is compared to the Network element in the Allow tag, followed by the Network element in the Deny tag. Then the request is compared with the Geo element in the Allow tag, followed by the Geo element in the Deny tag.



**Note** If the request is denied during the comparison with the Network element (either by not matching the Allow condition or by matching the Deny condition), no further comparison is performed even if the Geo element is defined.

**Deny, Allow**

If the Order tag is defined as <Deny, Allow>, and both the Network element and the Geo element are defined for both the Allow tag and the Deny tag, first the request is compared to the Network element in the Deny tag, followed by the Network element in the Allow tag. Then the request is compared with the Geo element in the Deny tag, followed by the Geo element in the Allow tag.

**Note**

If the request is denied during the comparison with the Network element (either by matching the Deny condition or by not matching the Allow condition), no further comparison is performed even if the Geo element is defined.

**Allow**

If the Order tag is only defined as Allow, and both the Allow tag and Deny tag are defined, the request is only compared with the Allow tag conditions. The Deny tag conditions are ignored. If the request does not match the Network element in the Allow tag, no further comparison is performed even if the Geo element is defined. If the request matches the Network element in the Allow tag, then the request is compared with Geo element next.

**Deny**

If the Order tag is only defined as Deny, and both the Allow tag and Deny tag are defined, the request is only compared with the Deny tag conditions. The Allow tag conditions are ignored. If the request matches the Network element in the Deny tag, no further comparison is performed even if the Geo element is defined.

## Order Scenarios

**Table D-2** lists the different Order tag settings and outcomes for single elements (Network or Geo) defined in each Allow and Deny tag, and multiple elements defined in each Allow and Deny tag. A reference to an XML example is provided for each scenario.

**Table D-2** *Geo/IP XML Order Scenarios*

Case	Order	Single Element	Multiple Elements
1	Allow, Deny	If Allow element does not match, deny the request. See <a href="#">Example 3, page D-7</a> .	If Allow Network element does not match, the request is denied and no further checking is performed. See <a href="#">Example 9, page D-9</a> .
2	Allow, Deny	If Allow element matches, allow the request. See <a href="#">Example 1, page D-6</a> .	If Allow Network element matches, check Allow Geo element. See <a href="#">Example 11, page D-10</a> .
3	Deny, Allow	If Deny element does not match, check Allow element and take action. See <a href="#">Example 4, page D-7</a> .	If Deny Network element does not match, check Allow Network element. If Allow Network element matches, check Deny Geo element. If Deny Geo element does not match, check Allow Geo element. If Allow Geo element matches, allow the request.  If at any point along the above checking path, the Deny element matches, or the Allow element does not match; the request is denied.
4	Deny, Allow	If Deny element matches, deny the request. See <a href="#">Example 2, page D-6</a> .	If Deny Network tag matches, request is denied. See <a href="#">Example 15, page D-12</a> .

## ■ Understanding the Allow and Deny Conditions

**Table D-2** Geo/IP XML Order Scenarios (continued)

Case	Order	Single Element	Multiple Elements
5	Allow	If Allow element does not match, deny the request. See <a href="#">Example 8, page D-9</a> .	First check the Allow Network element, if it is configured. Then check the Allow Geo element if it is configured. See <a href="#">Example 14, page D-12</a> .
6	Allow	If Allow element matches, allow the request. See <a href="#">Example 7, page D-8</a> . First check the Allow Network element, if more than one Network element is configured, check each one. See <a href="#">Example 16, page D-13</a> .	
7	Deny	If Deny element does not match, allow the request. See <a href="#">Example 6, page D-8</a> .	First check the Deny Network element, if it is configured. Then check the Deny Geo element if it is configured. See <a href="#">Example 13, page D-11</a> .
8	Deny	If Deny element matches, deny the request. See <a href="#">Example 5, page D-8</a> .	



**Note** The allowed or denied results for the following examples are based on a client IP address of 209.165.201.30, which for the purposes of these examples belongs to India.

### Example 1

The result in this example is that the client request is allowed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Service Provider Ultra-CDN</CustomerName>
    <Allow>
        <Pattern>*</Pattern>
        <Geo>
            <Country name="india" />
            <Line_speed>high</Line_speed>
            <Field name="postal_code" value="200000" />
            <Field name="time_zone" value="8" />
        </Geo>
    </Allow>
    <Deny>
        <Pattern>*</Pattern>
        <Geo>
            <Country name="ALL" />
        </Geo>
    </Deny>
    <Order>Allow,Deny</Order>
</CDSAuthorization>
```

### Example 2

The result in this example is that the client request is denied.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Service Provider Ultra-CDN</CustomerName>
    <Allow>
        <Pattern>*</Pattern>
        <Geo>
```

```

<Country name="india"/>
<Line_speed>high</Line_speed>
<Field name="postal_code" value="200000" />
<Field name="time_zone" value="8" />
</Geo>
</Allow>
<Deny>
<Pattern>*</Pattern>
<Geo>
<Country name="ALL"/>
</Geo>
</Deny>
<Order>Deny,Allow</Order>
</CDSAuthorization>

```

### Example 3

The result in this example is that the client request is denied.

```

<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
<Revision>1.0</Revision>
<CustomerName>Service Provider Ultra-CDN</CustomerName>
<Allow>
<Pattern>*</Pattern>
<Geo>
<Country name="united states"/>
<Line_speed>high</Line_speed>
<Field name="postal_code" value="200000" />
<Field name="time_zone" value="8" />
</Geo>
</Allow>
<Deny>
<Pattern>*</Pattern>
<Geo>
<Country name="ALL"/>
</Geo>
</Deny>
<Order>Allow,Deny</Order>
</CDSAuthorization>

```

### Example 4

The result in this example is that the client request is allowed.

```

<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
<Revision>1.0</Revision>
<CustomerName>Service Provider Ultra-CDN</CustomerName>
<Allow>
<Pattern>*</Pattern>
<Geo>
<Country name="ALL"/>
<Line_speed>high</Line_speed>
<Field name="postal_code" value="200000" />
<Field name="time_zone" value="8" />
</Geo>
</Allow>
<Deny>
<Pattern>*</Pattern>
<Geo>
<Country name="united states"/>
</Geo>

```

## ■ Understanding the Allow and Deny Conditions

```
</Deny>
<Order>Deny,Allow</Order>
</CDSAuthorization>
```

### Example 5

The result in this example is that the client request is denied.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Service Provider Ultra-CDN</CustomerName>
    <Allow>
        <Pattern>*</Pattern>
        <Geo>
            <Country name="ALL" />
            <Line_speed>high</Line_speed>
            <Field name="postal_code" value="200000" />
            <Field name="time_zone" value="8" />
        </Geo>
    </Allow>
    <Deny>
        <Pattern>*</Pattern>
        <Geo>
            <Country name="india" />
        </Geo>
    </Deny>
    <Order>Deny</Order>
</CDSAuthorization>
```

### Example 6

The result in this example is that the client request is allowed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Service Provider Ultra-CDN</CustomerName>
    <Allow>
        <Pattern>*</Pattern>
        <Geo>
            <Country name="ALL" />
            <Line_speed>high</Line_speed>
            <Field name="postal_code" value="200000" />
            <Field name="time_zone" value="8" />
        </Geo>
    </Allow>
    <Deny>
        <Pattern>*</Pattern>
        <Geo>
            <Country name="united states" />
        </Geo>
    </Deny>
    <Order>Deny</Order>
</CDSAuthorization>
```

### Example 7

The result in this example is that the client request is allowed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
```

```

<Revision>1.0</Revision>
<CustomerName>Service Provider Ultra-CDN</CustomerName>
<Allow>
    <Pattern>*</Pattern>
    <Geo>
        <Country name="india"/>
        <Line_speed>high</Line_speed>
        <Field name="postal_code" value="200000" />
        <Field name="time_zone" value="8" />
    </Geo>
</Allow>
<Deny>
    <Pattern>*</Pattern>
    <Geo>
        <Country name="united states"/>
    </Geo>
</Deny>
<Order>Allow</Order>
</CDSAuthorization>

```

### Example 8

The result in this example is that the client request is denied.

```

<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Service Provider Ultra-CDN</CustomerName>
    <Allow>
        <Pattern>*</Pattern>
        <Geo>
            <Country name="india"/>
            <Line_speed>high</Line_speed>
            <Field name="postal_code" value="200000" />
            <Field name="time_zone" value="8" />
        </Geo>
    </Allow>
    <Deny>
        <Pattern>*</Pattern>
        <Geo>
            <Country name="united states"/>
        </Geo>
    </Deny>
    <Order>Allow</Order>
</CDSAuthorization>

```

### Example 9

The result in this example is that the client request is denied.

```

<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Service Provider Ultra-CDN</CustomerName>
    <Allow>
        <Pattern>*</Pattern>
        <Network>127.0.0.1/32</Network>
        <Geo>
            <Country name="india"/>
            <Line_speed>high</Line_speed>
            <Field name="postal_code" value="200000" />
            <Field name="time_zone" value="8" />
        </Geo>
    </Allow>

```

## ■ Understanding the Allow and Deny Conditions

```

</Allow>
<Deny>
  <Pattern>*</Pattern>
  <Geo>
    <Country name="ALL" />
  </Geo>
</Deny>
<Order>Allow,Deny</Order>
</CDSAuthorization>

```

### Example 10

The result in this example is that the client request is allowed.

```

<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>209.165.201.0/27</Network>
    <Geo>
      <Country name="india" />
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Geo>
      <Country name="ALL" />
    </Geo>
  </Deny>
  <Order>Allow,Deny</Order>
</CDSAuthorization>

```

### Example 11

The result in this example is that the client request is denied. In the example below, first the Allow Network element is checked, which matches the client, so the intermediate result is the request is allowed, but the Allow Geo element is checked, which does not match the client request, so the final result is the request is denied.

```

<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>209.165.201.0/27</Network>
    <Geo>
      <Country name="india" />
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Geo>
      <Country name="ALL" />
    </Geo>
  </Deny>
</CDSAuthorization>

```

```

    </Geo>
  </Deny>
  <Order>Allow,Deny</Order>
</CDSAuthorization>
```

**Example 12**

The result in this example is that the client request is denied. In the example below, first the Allow Network element is checked, which does not match the client, so the request is denied. No further checking is performed.

```

<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>10.1.1.1/32</Network>
    <Geo>
      <Country name="india"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Network>1.1.1.1/32</Network>
    <Geo>
      <Country name="ALL"/>
    </Geo>
  </Deny>
  <Order>Allow,Deny</Order>
</CDSAuthorization>
```

**Example 13**

The result in this example is that the client request is denied. In the example below, first the Deny Network element is checked, which matches the client, so the request is denied. No further checking is performed.

```

<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>10.1.1.1/32</Network>
    <Geo>
      <Country name="united states"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Network>209.165.201.0/27</Network> --->Final result Deny (so don't process further)
    <Geo>
      <Country name="ALL"/>
    </Geo>
  </Deny>
</CDSAuthorization>
```

## ■ Understanding the Allow and Deny Conditions

```
<Order>Deny</Order>
</CDSAuthorization>
```

### Example 14

The result in this example is that the client request is denied. In the example below, first the Allow Network element is checked, which does not match the client, so the request is denied. No further checking is performed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>10.1.1.1/32</Network>
    <Geo>
      <Country name="united states"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Network>209.165.201.0/27</Network>
    <Geo>
      <Country name="ALL"/>
    </Geo>
  </Deny>
  <Order>Allow</Order>
</CDSAuthorization>
```

### Example 15

The result in this example is that the client request is denied. In the example below, first the Deny Network element is checked, which matches the client, so the request is denied. No further checking is performed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>10.1.1.1/32</Network>
    <Geo>
      <Country name="united states"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Network>209.165.201.0/27</Network>
    <Geo>
      <Country name="india"/>
    </Geo>
  </Deny>
  <Order>Deny,Allow</Order>
```

```
</CDSAuthorization>
```

**Example 16**

The result in this example is that the client request is allowed. In the example below, first the Allow Network element is checked, the client IP address only has to match one Network element, so even though the first two Network elements do not match, the third Network element does match and the client request is allowed. No further checking is performed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
<Revision>1.0</Revision>
<CustomerName>Service Provider Ultra-CDN</CustomerName>
<Allow>
<Pattern>*</Pattern>
<Network>10.1.1.1/32</Network>
<Network>10.2.2.2/32</Network>
<Network>209.165.201.0/27</Network>
</Allow>
<Deny>
<Pattern>*</Pattern>
<Geo>
<Country name="ALL"/>
</Geo>
</Deny>
<Order>Allow</Order>
</CDSAuthorization>
```

# Geo/IP File Examples

The following is an example of the Authorization Service configuration file example.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
<Revision>1.0</Revision>
<CustomerName>ACompany</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>
```

**Geo/IP File Examples**

```

<Deny>
  <Pattern>*</Pattern>
  <Geo>
    <Country name="france"/>
    <Country name="china">
      <State name="ALL">
      </State>
    </Country>
  </Geo>
</Deny>
<Order>Allow,Deny</Order>
</CDSAuthorization>

```

Following is an example of a Geo/Ip file with both IPv4 and IPv6 addresses:

```

<CDSAuthorization
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">

  <Revision>1.0</Revision>
  <CustomerName>Cisco Systems</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>1.1.1.1/24</Network>
    <Network>2001:0DB8:0000:0001::/64</Network>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Network>2.2.2.2/24</Network>
    <Network>2001:0DB8:0000:0002::/64 </Network>
  </Deny>
  <Order>Allow,Deny</Order>
</CDSAuthorization>

```



## Creating Service Rule Files

This appendix describes the Service Rule file used by a delivery service to specify the service rules for all the SEs in a delivery service. This appendix consists of the following topics:

- [Introduction, page E-1](#)
- [Service Rule File Structure and Syntax, page E-4](#)
- [Rule Actions for Web Engine, page E-12](#)
- [Rule Actions for Flash Media Streaming, page E-26](#)
- [URL Signing Key in the Service Rule File, page E-18](#)
- [Service Rule File Example, page E-31](#)



### Note

The Service Rule file is only supported for the Web Engine and Flash Media Streaming. Windows Media Streaming and Movie Streamer should continue to configure service rules by device. For more information, see the “[Configuring Service Rules](#)” section on page 4-21. For the Web Engine and Flash Media Streaming, the Service Rule file must be used if service rules are to be configured.

The Authorization Service must be enabled on all SEs participating in a delivery service that uses the Service Rule Configuration. The Authorization Service is enabled by default. For more information, see the “[Configuring the Authorization Service](#)” section on page 4-28.

When Geo/IP and service rules are configured by way of XML configuration files that are associated with a delivery service, each client request goes through the following processing order:

1. SE bypass (this is used for multi-tiered SEs), no configuration is required
2. Service rules
3. Geo/IP Network element
4. Geo/IP Geo element

For information about Geo/IP, see [Appendix D, “Creating Geo/IP Files.”](#)

## Introduction

The Service Rule file is an XML file used to specify the service rules for all the SEs in a delivery service. Just the same as configuring service rules for each SE, the Service Rule file allows you to specify a set of rules, each clearly identified by an action and a pattern, for all the SEs in a delivery service. Subsequently, for every incoming request, if a pattern for a rule matches the given request, the

corresponding action for that rule is taken. You do not need to enable Service Rules on each SE for the Web Engine and Flash Media Streaming, just create a Service Rule file, upload it to the VDS, and assign it to the delivery service.



**Note** In a Service Rule File, you can define multiple PatternListGrps.

It is not recommended that you use a single Service Rule File for several Delivery Services, since a single request belongs to a specified delivery service. It will cost more CPU cycles while going through all the PatternListGrps and all the other rules defined later, that is not applied to the delivery service.

## Converting Old Service Rules to New Service Rules

The following example shows the commands for configuring a service rule that performs a URL rewrite using the old mechanism:

```
SE (config)# rule enable
SE (config)# rule action rewrite pattern-list 1
SE (config)# rule pattern-list 1 url-regsub http://.*.rfqdn2.cds.cisco.com/(.*)
http://$1
```

The Service Rule XML file for the above rule is as follows:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>MOD</CustomerName>
<Rule_Patterns>
    <PatternListGrp id = "grp1">
        <UrlRegex>.rfqdn2.cds.cisco.com/</UrlRegex>
    </PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
    <Rule_Allow matchGroup = "grp1" protocol = "http" />
    <Rule_UrlRewrite matchGroup = "grp1" protocol = "http" regsub = "http://.*.rfqdn2.cds.cisco.com/(.*)" 
rewrite-url = "http://$1" />
</Rule_Actions>
</CDSRules>
```

**Table E-1** shows the mapping between a service rule pattern command and an XML pattern.

**Table E-1 Mapping Service Rule Patterns—CLI Format to XML Format**

Pattern Type	CLI Pattern	XML Pattern
Domain	rule pattern-list 1 domain rfqdn.cds.com	<PatternListGrp id = "1"> <Domain>rfqdn.cds.com</Domain> </PatternListGrp>
SrcIp	rule pattern-list 1 src-ip 1.1.1.1 255.255.255.0	<PatternListGrp id = "1"> <SrcIp>1.1.1.1</SrcIp> </PatternListGrp>
UrlRegex	rule pattern-list 2 url-regex http:\V.*.svc01.cdn.t-online.de\web[0-9]+\\streaming\\CDN_testprovider_2\\streaming\\.*	<PatternListGrp id = "2"> <UrlRegex> http:\V.*.svc01.cdn.t- online.de\web[0-9]+\\streaming\\CDN_testprovider_2\\streaming\\.* </UrlRegex> </PatternListGrp>

The pattern type header-field is not supported in the Service Rule file.

**Table E-2** shows the mapping between a service rule action command and an XML action.

**Table E-2 Mapping Service Rule Actions—CLI Format to XML Format**

Action Type	CLI Action	XML Action
Allow	rule action allow pattern-list 1 protocol http	<Rule_Allow matchGroup = "1" protocol = "http" />
Block	rule action block pattern-list 2 protocol http	<Rule_Block matchGroup = "2" protocol = "http" />
Validate	rule action validate-url-signature error-redirect-url "http://wwwin.cisco.com" pattern-list 1 protocol http	<Rule_Validate matchGroup = "1" protocol = "http" error-redirect-url = "http://wwwin.cisco.com" exclude-validation = "all" />
UrlRewrite	rule pattern-list 3 url-regsub http://(.*)cdsis.com/(.*)mp4(.*) http://customer.com/%29%28(.*) http://\$1\$2\$3mp4 rule action rewrite pattern-list 3 protocol http	<Rule.UrlRewrite matchGroup = "3" protocol = "http" regsub = "http://(.*)cdsis.com/(.*)mp4(.*)" http://customer.com/%29%28(.*)" rewrite-url = " http://\$1\$2\$3mp4" />

## Adding a Service Rule File to the VDS

The Service Rule files can be created using any ASCII text-editing tool. The Service Rule file are registered to the VDS by using the Authorization File Registration page. For more information see the “Authorization File Registration” section on page 6-15. When the file has been registered, you can assign it to a delivery service through the Authorization Plugins page. For more information, see the “Authorization Plugins” section on page 5-27.

# Service Rule File Structure and Syntax

The XML Schema file describes and dictates the content of the XML file. The CDSRules.xsd file contains the XML schema. To view or download a copy of the CDSRules.xsd file, see the “[Viewing or Downloading XML Schema Files](#)” section on page 6-24.

**Table E-3** defines the Service Rule file elements. For more information on the rule actions supported by Web Engine, see the “[Rule Actions for Web Engine](#)” section on page E-12. For more information on the rule actions supported by Flash Media Streaming, see the “[Rule Actions for Flash Media Streaming](#)” section on page E-26.

**Table E-3** *Service Rule File Elements*

Element	Subelements	Attributes	Description
CDSRule	Revision		Optional. Revision number to specify the version of this file.
	CustomerName		Optional. Customer name associated with this file.
	ApplyAllTier		Required for the Rule.UrlResolve rule action.
	Rule_Patterns		Patterns to match for a specified action. There can be only one Rule_Patterns element for a Service Rule file.
	Rule_Actions		Action to take when a pattern is matched. There can be only one Rule_Actions element for a Service Rule file.
ApplyAllTier			<p>Valid values for the ApplyAllTier element are “yes” or “no.”</p> <p>The ApplyAllTier element has the following effect:</p> <ul style="list-style-type: none"> <li>If the ApplyAllTier is set to “yes,” the Rule.UrlResolve rule action is applied to all SEs in the delivery service. The ApplyAllTier element must be set to “yes” for the Rule.UrlResolve to work properly. For more information, see the “<a href="#">URL Resolve</a>” section on page E-12.</li> <li>If the ApplyAllTier is set to “no” or if it is absent, and Rule.UrlResolve is included in the Service Rule file, the Rule.UrlResolve does not work properly.</li> <li>If the ApplyAllTier is set to “no” or if it is absent, and Rule.UrlResolve is not included, the Service Rule file is only applied to the edge tier.</li> <li>If the Service Rule file needs to be applied to the Content Acquirer (root SE), then ApplyAllTier must be set to “yes.”</li> </ul>
Rule_Patterns	PatternListGrp		Marks the beginning and ending of all the defined patterns in this file.
PatternListGrp	Domain SrcIp UrlRegex	id	<p>The PatternListGrp <i>id</i> attribute is used to identify the pattern list group and can be up to 128 alphanumeric characters.</p> <p><b>Note</b> Currently, the Header element is not supported.</p>

**Table E-3** Service Rule File Elements (continued)

Element	Subelements	Attributes	Description
Domain			<p>The Domain element is used to match the domain name in the URL or the host header against a regular expression. For more information, see the <a href="#">Table 4-12 on page 4-23</a>.</p> <p><b>Note</b> When VOD (prefetch/caching) and live streaming share the same content origin, and the Service Rules XML file is configured to validate the signed URL where the domain must match the Service Routing Domain Name, make sure to create rule patterns for the URL validation to match both the Service Routing Domain Name and the Origin Server FQDN. Additionally, when the URL is signed, exclude the domain from the signature. See the <a href="#">“Running a Python URL Signing Script” section on page H-11</a> for more information. The URL validation must not include the domain for validation (use the <b>exclude-domain</b> option for the <i>exclude-validate</i> attribute of the Rule_Validate element).</p>
SrcIp			Matches the source IP address of the request. The SrcIP pattern requires the IP address be specified in the classless inter-domain routing (CIDR) format. The Service Rule XML file validation fails if the IP address is not in CIDR format.
UrlRegex			<p>Matches the URL against a regular expression. The match is case sensitive. The following example covers both uppercase and lowercase expressions of MP4 files:</p> <pre>&lt;UrlRegex&gt; http://.*.cdsis.com/.*.[mM][pP]4 &lt;/UrlRegex&gt;</pre> <p><b>Note</b> The VDS-IS system uses GNU regular expressions.</p>
Rule_Actions	Rule_Allow Rule_Block Rule_Validate Rule.UrlRewrite Rule_NoCache Rule.UrlRedirect Rule.UrlResolve Rule.UrlGenerateSign Rule_ForceRevalidate Rule_SwfFileValidate Rule_Dscp Rule_SetAction		For information about the rule action processing, see the <a href="#">“Rule Action Processing” section on page E-11</a> .

**Table E-3** Service Rule File Elements (continued)

Element	Subelements	Attributes	Description
Rule_Allow		matchGroup protocol	The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be one or more of the following: http, rtmp, rtmpe, rtmpmt, and rtmpme.
Rule_Block		matchGroup protocol	The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be one or more of the following: http, rtmp, rtmpe, rtmpmt, and rtmpme.
Rule_Validate		matchGroup protocol error-redirect-url exclude-validation key public-key symmetric-key	<p>The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be one or more of the following: http, rtmp, rtmpe, rtmpmt, and rtmpme.</p> <p>The <i>error-redirect-url</i> attribute value is the URL that clients are redirected to if they fail validation.</p> <p>The <i>exclude-validation client-ip</i> attribute instructs the SEs to ignore the client's IP address when processing the validation of the signed URL.</p> <p>The <i>exclude-validation expiry-time</i> attribute instructs the SEs to ignore the expiry time that normally limits access to the content when the expiry time has occurred.</p> <p>The <i>exclude-validation exclude-domain</i> attribute instructs the SEs to ignore the domain in the URL when processing the validation of the signed URL.</p> <p>The <i>exclude-validation all</i> attribute instructs the SEs to ignore both the client IP address and the content expiration time when processing the validation of the signed URL.</p> <p>The key, public-key, and symmetric-key attributes are described in the “<a href="#">URL Signing Key in the Service Rule File</a>” section on page E-18.</p>

**Table E-3** Service Rule File Elements (continued)

Element	Subelements	Attributes	Description
Rule.UrlRewrite		matchGroup protocol rewrite-url regsub	<p>The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be http.</p> <p><b>Note</b> Only http is supported as the <i>protocol</i> attribute value All other values have no affect.</p> <p>The <i>rewrite-url</i> attribute value is the URL used to rewrite the original request.</p> <p>The <i>regsub</i> attribute value is the regular expression the request URL must match to be replaced with the <i>rewrite-Url</i> attribute value. The regsub attribute value must be an exact match of the string you want to replace in the request URL.</p> <p><b>Note</b> The regsub attribute supports regular expressions, but only one substitution is supported per Rule.UrlRewrite. Multiple substitutions for the same Rule.UrlRewrite are not supported.</p>
Rule.NoCache		matchGroup protocol	<p>The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be http.</p> <p><b>Note</b> Only http is supported as the <i>protocol</i> attribute value All other values have no affect.</p>
Rule.UrlRedirect		matchGroup protocol redirect-url	<p>The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be http. The <i>redirect-url</i> attribute value is the URL to redirect the request to.</p> <p><b>Note</b> Only http is supported as the <i>protocol</i> attribute value All other values have no affect.</p>

**Table E-3** Service Rule File Elements (continued)

Element	Subelements	Attributes	Description
Rule_UrlResolve		matchGroup protocol	The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be http.  <b>Note</b> Only http is supported as the protocol attribute value. All other values have no affect.
	SourceUrl (required)	regsub rewrite-url	The <i>regsub</i> attribute value is the regular expression the request URL must match to be replaced with the <i>rewrite-Url</i> attribute value. The <i>regsub</i> attribute value must be an exact match of the string you want to replace in the request URL.  <b>Note</b> The <i>regsub</i> attribute supports regular expressions, but only one substitution can be defined. Multiple substitutions are not supported.  The <i>rewrite-url</i> attribute value is the URL used to rewrite the original request.
	StorageUrl (required)	regsub rewrite-url	The <i>regsub</i> attribute value is the regular expression the request URL must match to be replaced with the <i>rewrite-Url</i> attribute value. The <i>regsub</i> attribute value must be an exact match of the string you want to replace in the request URL.  <b>Note</b> The <i>regsub</i> attribute supports regular expressions, but only one substitution can be defined. Multiple substitutions are not supported.  The <i>rewrite-url</i> attribute value is the URL used to rewrite the original request.

**Table E-3** Service Rule File Elements (continued)

Element	Subelements	Attributes	Description
Rule.UrlGenerateSign		matchGroup protocol key-id-owner key-id-number timeout-in-sec key private-key symmetric-key	<p>The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be http.</p> <p>The <i>key-id-owner</i> attribute value is the ID number for the owner of the encryption key. Valid entry is 1 if the key is defined in the Service Rule XML file. Valid entries are from 1 to 32 if the key is defined in the URL Signing page or by using the <b>url-signature</b> command.</p> <p>The <i>key-id-number</i> attribute value is the encryption key ID number. Valid entry is 1 if the key is defined in the Service Rule XML file. Valid entries are from 1 to 16 if the key is defined in the URL Signing page or by using the <b>url-signature</b> command.</p> <p>The <i>timeout-in-sec</i> attribute value is the time interval to wait before expiring the signed URL. The default is 30 seconds.</p> <p><b>Note</b> Only http is supported as the <i>protocol</i> attribute value All other values have no affect.</p> <p>The key, private-key, and symmetric-key attributes are described in the “URL Signing Key in the Service Rule File” section on page E-18.</p>
Rule.ForceRevalidate		matchGroup protocol	<p>The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be http.</p> <p><b>Note</b> Only http is supported as the <i>protocol</i> attribute value All other values have no affect.</p>
Rule.SwfFileValidate		matchGroup protocol	The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be one or more of the following: rtmp, rtmpe, rtmpt, and rtmpte.
Rule.Dscp		matchGroup protocol dscp-bits	The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes. The <i>protocol</i> attribute value must be one or more of the following: rtmp, rtmpe, rtmpt, and rtmpte. The <i>dscp-bits</i> attribute value ranges from 0 to 63. Absence of the tag in the rules xml file shall assume default DSCP value to 0.
Rule_SetAction	SetParameter SetRewrite SetExecute		The Rule_SetAction is used for Session-Based Encryption and Session Tracking. For more information, see <a href="#">Appendix F, “ABR Session-Based Encryption and Session Tracking.”</a>

All specified attributes for the Rule\_Actions subelements are required, except the exclude-validation attribute, which is optional.

## Pattern Matching

Before any pattern matches are checked, the protocol is checked. If the protocol of the incoming request does not match the protocols specified for the rule action, the action is not taken. If a pattern for a rule matches the given request, the corresponding action for that rule is taken.

### Boolean AND Function

When a PatternListGrp is specified for an action, it implies an AND of all the patterns within the group. All patterns specified in that group must be matched for the action to take place. In the following example, both patterns in grp1 must be matched for the action to be taken.

```
<Rule_Patterns>
    <PatternListGrp id = "grp1">
        <Domain>fmsvod.com</Domain>
        <uRLregex>clouds</uRLregex>
    </PatternListGrp>
</Rule_Patterns>
```

### Boolean OR Function

When the matchGroup id attributes are separated by a comma, it implies an OR of all the patterns. The action is taken when either of the patternListGrp elements are matched. In the following example, the pattern of either grp1 or grp2 is considered a match.

```
<Rule_Patterns>
    <PatternListGrp id = "grp1">
        <Domain>fmsvod.com</Domain>
    </PatternListGrp>
</Rule_Patterns>
<Rule_Patterns>
    <PatternListGrp id = "grp2">
        <uRLregex>clouds</uRLregex>
    </PatternListGrp>
</Rule_Patterns>

<Rule_Actions>
    <Rule_Block matchGroup = "grp1,grp2" protocol = "rtmp" />
</Rule_Actions>
```

In the following example, multiple protocols are specified for the same rule by including the protocols separated by a comma as a value of the protocol attribute:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Capricious</CustomerName>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <Domain>fmsvod.com</Domain>
        </PatternListGrp>
    </Rule_Patterns>

    <Rule_Actions>
        <Rule_Validate matchGroup = "grp1" protocol = "rtmpe,rtmpte"
            error-redirect-url="http://www.cisco.com"/>
    </Rule_Actions>
</CDSRules>
```

## Rule Action Processing

The rules are processed in the same order they are listed in the Rule\_Actions element.

Multiple Rule\_Actions can be configured; for example, there can be a Rule\_Allow followed by a Rule\_Block followed by a Rule\_UrlRewrite and so on. The Rule\_Actions can be in any order and the processing of the rules is determined by the order they are listed in the Service Rule XML file.

The maximum number of rule actions allows is 100. If the number of rule actions exceeds 100, then the Service Rule XML file validation fails.

**Note**

For RTSP, rules processing uses the Rule daemon and not the Authsvr process; therefore, the authsvr statistics (**show statistics authsvr delivery-service-id <delivery service ID> rules**) are not incremented. For HTTP, if ApplyAllTier is set to "no," statistics are incremented only on the edge SE, not the Content Acquirer (root SE).

Only the following rule actions are allowed to have multiple entries:

- Rule\_Rewrite
- Rule\_UrlResolve
- Rule\_UrlGenerateSign

All other rule actions can only have a single entry. If there are multiple entries of the same Rule\_Actions subelement, the last entry with a matched condition is the rule that is applied.

The following list describes the Rule\_Actions processing:

- When a Rule\_Allow pattern is matched, the request is allowed, and if there are subsequent rules, the next Rule\_Actions is processed. If the condition is not matched, the request is denied and no further rule processing is performed.
- When a Rule\_Block pattern is matched, the request is blocked and the Rule\_Actions processing does not continue.
- When a Rule\_Validate pattern is matched, the request is validated and if the validation is successful, the Rule\_Actions processing continues to the next rule configured. If the validation fails, the request is not validated and the Rule\_Actions processing stops. For more information about rule processing for Rule\_Validate, see the [“Service Rule Action Order for Rule\\_Validate and Rule\\_UrlGenerateSign” section on page E-22](#).
- Whether a Rule\_UrlRewrite pattern is matched or not, rule processing continues to the next configured rule. If the Rule\_UrlRewrite pattern is matched, the request is rewritten. If the Rule\_UrlRewrite pattern is not matched, the request is not rewritten.
- Whether a Rule\_NoCache pattern is matched or not, rule processing continues to the next configured rule. Rule\_NoCache action just determines whether to cache the content on the SE or not, provided further rule processing results in the request being allowed. If the Rule\_NoCache pattern is matched, the content is not cached on the SE. If the Rule\_NoCache pattern is not matched, the content is cached on the SE.
- Whether a Rule\_UrlRedirect pattern is matched or not, rule processing continues to the next configured rule. If the Rule\_UrlRedirect pattern is matched, the request is redirected. If the Rule\_UrlRedirect pattern is not matched, the request is not redirected.
- Whether a Rule\_UrlResolve pattern is matched or not, rule processing continues to the next configured rule. Rule\_UrlResolve action maps the incoming URL to a Source and Storage URL Source URL. If the Rule\_UrlResolve pattern is not matched, the mapping does not occur.

## ■ Rule Actions for Web Engine

- When a Rule.UrlGenerateSign pattern is matched, a generated URL signature is returned to the client as part of the ASX response for Windows Media Streaming live programs, and processing continues to the next configured rule. For more information about the rule process for the Rule.UrlGenerateSign rule action, see the “[Windows Media Streaming ASX Files with URL Signing](#)” section on page E-20.
- Whether a Rule.ForceReValidate pattern is matched or not, rule processing continues to the next configured rule. Rule.ForceReValidate action enables the Web Engine to take the appropriate revalidation action. If the Rule.ForceReValidate pattern is not matched, the revalidation action is not taken.
- Whether a Rule.SwfFileValidate is matched or not, rule processing continues to the next configured rule. Rule.SwfFileValidate action enables Flash Media Streaming to perform SWF file validation. If the Rule.SwfFileValidate pattern is not matched, the SWF file is not validated.

# Rule Actions for Web Engine

The service rule actions for allow, block, URL signature validation, URL rewrite, and no cache are described at the beginning of the [Creating Service Rule Files](#) appendix. This section provides details on the following rule actions:

- [URL Resolve](#)
- [URL Redirect](#)
- [Force Revalidation](#)
- [URL Generate Signature](#)

As well as information on converting Windows Media Streaming service rules for generate-url-signature and validate-url-signature (“[Converting Old Windows Media Streaming Service Rules for URL Signing and Validation](#)” section on page E-25).

### Multiple Rule Actions in Web Engine

It is important to note that the Web Engine only applies one of the following rule actions, in the following order:

1. Rule.UrlRedirect
2. Rule.UrlResolve
3. Rule.UrlRewrite

If more than one rule action is returned from the Authorization Server, only the one with the higher priority is chosen.

## URL Resolve

In many content delivery cases, URLs are not just used as unique identifiers of the content, but they are also used to transfer specialized information from the client to the Origin Servers (for example, client IP address es and special tags for video identification) in the form of query strings.

The URL Resolve rule action (Rule.UrlResolve) provides a way to take a client’s incoming URL (known as the Intercept URL) and resolve it into other URLs that can be used for caching (known as the Storage URL) and ingesting the content (known as the Source URL).

**Note** The default behavior of the Web Engine is to cache the content when the request URL has a query string, which results in multiple copies of the same content being stored. The Rule\_NoCache rule action in the Service Rule file offers a way to not cache content with query strings; however, this meant the content was served by way of bypass (downloaded from the Origin Server directly), which resulted in more connections to the Origin Server. With the Rule\_UrlResolve rule action, the Storage URL provides a way to address any URL uniqueness that complicates caching, so long as the uniqueness can be removed by parsing the URL and replacing parts of the URL with regular expressions.

Table E-4 describes the URLs used in Rule\_UrlResolve and the CDS-Domain header.



**Note**

URL Resolve Rule does not work when ABR Session Tracking is enabled. For more information on HLS Session Tracking, see the [Appendix F, “ABR Session-Based Encryption and Session Tracking.”](#)

**Table E-4 Components of the URL Resolve**

Component	Description
Intercept URL (required)	Incoming URL from the client or downstream proxy. This is the URL that the client uses to send a request for content. This URL has the domain name that matches the service routing fully-qualified domain name (RFQDN). The Service Router, or other device in the DNS plane, can redirect and resolve the request to a device that is part of the service routing domain and that serves the content. The Intercept URL is seen by the SE in the following form:  <code>http://SE-HOST-NAME.se.Service_Routing_Domain_Name/Content_Path</code>
Storage URL (required)	Translated URL used by the Web Engine for storage-related operations. This is the URL used to store and locate the content on the SEs. Typically, this is the same as the Source URL. However, this URL can be any configured regular expression. The Storage URL has the following form:  <code>http://origin_server/Content_Path</code>  <b>Note</b> Required subelement of the Rule_UrlResolve rule action.  <b>Note</b> Cisco recommends that the domain should be either the Origin Server fully-qualified domain name (OFQDN) or the RFQDN of the delivery service. When the domain of the Storage URL is configured to be something other than the OFQDN of the delivery service to which the request belongs, dynamically cached content is not deleted from the SE when the SE is unassigned from the delivery service. Content deletion only happens through the eviction process or by using the <b>clear content</b> command.

**Table E-4 Components of the URL Resolve (continued)**

Component	Description
Source URL (required)	<p>Translated URL used by the Web Engine to ingest content. This is the URL used to ingest content from the Origin server. Normally, the domain name of the incoming URL is replaced with the OFQDN. However, this URL can be any configured regular expression. The Source URL has the following format:</p> <pre>http://origin_server/Content_Path</pre> <p><b>Note</b> Configuring the Source URL domain to be the RFQDN of a delivery service causes the request to be rejected, because the RFQDN of a delivery service most likely resolves to the SR, which could result in loops in the system.</p> <p><b>Note</b> Required subelement of the Rule.UrlResolve rule action.</p>
CDS-Domain	<p>RFQDN of the delivery service to which the Intercept URL from the client belongs. The CDS-Domain header is sent from the downstream SE to the upstream SE.</p> <p>To ensure consistency in locating the SEs that are participating in the delivery service, the RFQDN is used in the URL sent from the edge SE to the middle-tiered SEs when a cache-miss occurs at the edge SE.</p> <p>When the middle-tiered SEs see the CDS-Domain header in the request, it replaces the domain in the “Intercept URL” (which is the edge SE’s Storage URL) with the RFQDN.</p> <p><b>Note</b> The CDS-Domain header is always sent, whether URL Resolve is configured or not. If this header is received from an end client, the request is rejected.</p>

**Example 1 Example for One-Tiered VDS**

This section provides an example of the Service Rule XML file with the Rule.UrlResolve rule action. The following parameters are used in the example:

- RFQDN—ott.c.awebsite.com
- OFQDN—cds.c.awebsite.com
- Origin Server—cache12.awebsite.com

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>DMZ1</CustomerName>
<Rule_Patterns>
    <PatternListGrp id = "grp1">
        <UrlRegex>ott.c.awebsite.com/.*/?params=(.*)</UrlRegex>
    </PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
    <Rule.UrlResolve matchGroup="grp1" protocol="http">
        <SourceUrl regsub="http://(.*)ott.c.awebsite.com/(.*)(params=)(.*)">
            rewrite-url="http://$1$2$3"/>
        <StorageUrl regsub="http://*.c.awebsite.com/(id=[0-9a-zA-Z]*)">
            rewrite-url="http://cds.c.awebsite.com/$1"/>
        </Rule.UrlResolve>
    </Rule_Actions>
</CDSRules>
```

The bold portion shows the regular expressions used to translate the Intercept URL into the Storage URL and the Source URL. The URL Resolve process for this example is as follows:

1. The client URL request (incoming URL) might be as follows:

```
http://ott.c.awebsite.com/cache12.awebsite.com/xaa?params=sparams=id&&ip=1.2.3.4&id=abcd
```

- After Service Router redirection, the URL request arrives at the edge SE in the Intercept URL form as follows:

```
http://sel.se.ott.c.awebsite.com/cache12.awebsite.com/xaa?params=sparams=id&ip=1.2.3.4&id=abcd
```

- After the Rule\_UrlResolve action, the following Source URL and Storage URLs are created:

Storage URL: <http://cds.c.awebsite.com/xaa?id=abcd>

Source URL: <http://cache12.awebsite.com/xaa?sparams=id&ip=1.2.3.4&id=abcd>

The following rules apply for URL Resolve:

- Only http is supported as the protocol attribute value, and only for VOD (prefetched, dynamic, and hybrid content), live, and adaptive bit rate (ABR). MP3 is not supported.
- Client headers (such as cookies, accept, and so on) are not forwarded to the origin server.
- If the Source URL belongs to another delivery service, processing continues to use the original delivery service.

#### **Example 2      Example for VDS with Two or More Tiers**

The basic example in the [Example 1 on page E-14](#) assumes a VDS with only one tier (root location). For systems with two tiers or more, there needs to be at least two Rule\_UrlResolve rules per delivery service:

- One to translate the Intercept URL coming from the SR to the edge tier.

```
http://sel.se.ott.c.awebsite.com/cache12.c.awebsite.com/videoplayback?params=sparams=id&ip=1.2.3.4&id=abcd
```

- Another to translate the Intercept URL coming from the edge tier to the middle tiers, which in this case, is actually the Source URL from the edge tier.

```
http://cache12.c.awebsite.com/videoplayback?params=id&ip=1.2.3.4&id=abcd
```

It is clear that the Intercept URL coming into the middle tiers does not match pattern grp1 in [Example 1 on page E-14](#). A second Rule\_UrlResolve rule action is required. The pattern for grp2 in the following Service Rule file example matches the Intercept URL coming into the middle tiers and will be translated into the same Source URL and Storage URL as the edge tier:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>DMZ1</CustomerName>
<ApplyAllTier>yes</ApplyAllTier>
<Rule_Patterns>
    <PatternListGrp id = "grp1">
        <UrlRegex>ott\.\c\.awebsite\.com/.*\?params=</UrlRegex>
    </PatternListGrp>
    <PatternListGrp id = "grp2">
        <UrlRegex> cache12.c.awebsite.com/.*\?params=</UrlRegex>
    </PatternListGrp>
    <Rule_Patterns>
        <Rule_UrlResolve matchGroup="grp1" protocol="http">
            <SourceUrl regsub="http://.*ott\.\c\.awebsite\.com/(.*\?)params=(.*)" rewrite-url="http://$1$2"/>
        </Rule_UrlResolve>
    </Rule_Patterns>
</Rule_Patterns>
<Rule_Actions>
    <Rule_UrlResolve matchGroup="grp1" protocol="http">
        <SourceUrl regsub="http://.*ott\.\c\.awebsite\.com/(.*\?)params=(.*)" rewrite-url="http://$1$2"/>
    </Rule_UrlResolve>
</Rule_Actions>
</CDSRules>
```

## ■ Rule Actions for Web Engine

```

<StorageUrl regsub="http://.*\c\awebiste\.com/(.*\?).*(id=[0-9a-zA-Z]*)"
    rewrite-url="http://cds.c.awebiste.com/$1$2"/>
</Rule_UrlResolve>

<Rule_UrlResolve matchGroup="grp2" protocol="http">
    <SourceUrl regsub="http://(.*)"
        rewrite-url="http://$1"/>
    <StorageUrl regsub="http://.*\c\awebiste\.com/(.*\?).*(id=[0-9a-zA-Z]*)"
        rewrite-url="http://cds.c.awebiste.com/$1$2"/>
</Rule_UrlResolve >
</Rule_Actions>
</CDSRules>
```

Additionally, this Service Rule file must be applied to every tier in the VDS to create the correct Source URL and Storage URL at each tier. The **ApplyAllTier** is a new Service Rule element that ensures the Service Rule file is applied to all tiers of the delivery service.



**Note** The **ApplyAllTier** element must be set to yes for the **Rule\_UrlResolve** to work properly.

### URL Rewrite and URL Resolve

URL Rewrite and URL Resolve have the following differences:

- URL Resolve (**Rule\_UrlResolve**) allows the configuration of separate Source and Storage URLs for a given incoming URL; URL Rewrite (**Rule\_UrlRewrite**) allows the Intercept URL to be modified and the modified URL is used for both the Source URL and Storage URL.
- Rule processing is different. In the case of **Rule\_UrlRewrite**, if the domain of the rewritten URL maps to a new delivery service, that delivery service is used to process the request. In the case of **Rule\_UrlResolve**, even if the domain of the Source URL maps to another delivery service, the original delivery service is used to process the request.

### Monitoring

Use the following commands to monitor the URL Resolve:

- **show statistics web-engine detail**
- **show cache content**
- **show cache-router routes web-engine URL**

The following new tokens have been added to the Web Engine custom log formats:

- %g—Storage URL
- %G—Source URL

The Web Engine Ingest log has a new field called CDS-Domain which has the CDS-Domain header being sent to the upstream SEs.

The **show statistics web-engine** command has a neVDSw counter, Authorization Resolve, which keeps track of the number of URL Resolve hits.

The **web-engine-error-logs** has a log entry of the Storage URL and Source URL. The log entry is identified by the WEUrl\*is string.

## URL Redirect

The URL Redirect (Rule.UrlRedirect) rule action is supported in the Service Rule XML file for the Web Engine. Following is an example of the Rule.UrlRedirect rule action:

```
<Rule.UrlRedirect matchGroup = "grp4" protocol = "http" redirect-url = "http://www.google.com" />
```

Whether a Rule.UrlRedirect pattern is matched or not, rule processing continues to the next configured rule. If the Rule.UrlRedirect pattern is matched, the request is redirected. If the Rule.UrlRedirect pattern is not matched, the request is not redirected.

The **show statistics web-engine** command has a new counter, Authorization Redirect, which keeps track of the number of URL Redirect hits.

## Force Revalidation

The Force Revalidation (Rule.ForceReValidate) action rule forces revalidation of cached content. The freshness of content algorithm and the comparison between the Origin Server expiry time with the max age value are ignored if this rule action is invoked.

If the Rule.ForceReValidate rule action is configured as part of Service Rule file, the Authorization Server responds to the Web Engine with the Rule.ForceReValidate directive. This enables the Web Engine to take appropriate revalidation action.

Following is an example of the Service Rule file with the Rule.ForceReValidate rule action:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>Cisco</CustomerName>
<Rule_Patterns>
    <PatternListGrp id = "grp1">
        <Domain>demo.cdsis.com</Domain>
    </PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
    <Rule_ForceReValidate matchGroup = "grp1" protocol = "http" />
</Rule_Actions>
</CDSRules>
```

Whether a Rule.ForceReValidate pattern is matched or not, rule processing continues to the next configured rule. Rule.ForceReValidate action enables the Web Engine to take the appropriate revalidation action. If the Rule.ForceReValidate pattern is not matched, the revalidation action is not taken.

The **show statistics web-engine** command has a new counter, Authorization Force Revalidate, which keeps track of the number of forced revalidation hits.

## URL Generate Signature

The URL Generate Signature (Rule.UrlGenerateSign) rule action is supported in the Service Rule XML file for the Web Engine. The Rule.UrlGenerateSign is a rule action for generating the URL signatures in the Windows Media metafile (ASX file) response associated with prefetched content, based on the SE configuration for the URL signature and this rule action.

## ■ Rule Actions for Web Engine

The Windows Media player receives the ASX file containing the signed URL, parses it, and sends out the request again with the signed URL. The SE receives the signed URL and performs the URL validation with the internally signed URL. If the validation is successful, the content is served to the client.

The Rule.UrlGenerateSign has the following attributes:

- matchGroup—Attribute value is the list of PatternListGrp *id* attributes
- protocol—Attribute value must be http
- key-id-owner—Attribute value is the ID number for the owner of the encryption key. Valid entry is 1 if the key is defined in the Service Rule XML file. Valid entries are from 1 to 32 if the key is defined in the URL Signing page or by using the **url-signature** command.
- key-id-number—Attribute value is the encryption key ID number. Valid entry is 1 if the key is defined in the Service Rule XML file. Valid entries are from 1 to 16 if the key is defined in the URL Signing page or by using the **url-signature** command.
- timeout-in-sec—Attribute value is the time interval to wait before expiring the signed URL. The default is 30 seconds.
- key—Unique URL signature key that is up to 16 characters. For symmetric key URL validation.
- private-key—URL where the private key file is located. For asymmetric key URL validation.
- symmetric-key—Key (16 bytes) used for AES encryption of the signed URL. For asymmetric key URL validation.



### Note

---

Only http is supported as the *protocol* attribute value. All other values have no affect.

---

Following is an example of the Service Rule file with the Rule.UrlGenerateSign rule action and the URL signing key defined in the URL Signing page:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Cisco</CustomerName>
    <ApplyAllTier>yes</ApplyAllTier>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <Domain>cisco.co</Domain >
        </PatternListGrp>
    </Rule_Patterns>

    <Rule_Actions>
        <Rule.UrlGenerateSign matchGroup = "grp1" protocol = "http" key-id-owner="1"
key-id-number="2" timeout-in-sec="30"/>
    </Rule_Actions>
</CDSRules>
```

## URL Signing Key in the Service Rule File

The Service Rule XML file supports URL signing configuration of symmetric and asymmetric keys. Additionally, URL signature validation is supported for all protocol engines, except Movie Streamer, and URL signature generation is supported for Windows Media Streaming live requests (.asx).

URL signing can still be configured for each SE by using the URL Signing page to specify the key parameters. If there are no key parameters specified in the Service Rule XML file, the SE settings are used. For more information on SE configuration, see the “[Configuring URL Signing Key](#)” section on page 4-27.

For information on converting Windows Media Streaming service rules for URL signature generation and validation with URL signing parameters, see the “[Converting Old Windows Media Streaming Service Rules for URL Signing and Validation](#)” section on page E-25.

The following new attributes have been added to the Rule\_Validate element:

- key—Unique URL signature key that is up to 16 characters. For symmetric key URL validation.
- public-key—URL where the public key file is located. For asymmetric key URL validation.
- symmetric-key—Key (16 bytes) used for AES encryption of the signed URL. For asymmetric key URL validation.

The following new attributes have been added to the Rule.UrlGenerateSign:

- key—Unique URL signature key that is up to 16 characters. For symmetric key URL validation.
- private-key—URL where the private key file is located. For asymmetric key URL validation.
- symmetric-key—Key (16 bytes) used for AES encryption of the signed URL. For asymmetric key URL validation.

The key ID owner and key ID number fields apply to the per-device configuration of URL Signing ([Devices > Devices > Service Control > URL Signing](#)). For compatibility, key ID owner and key ID number are required for the Rule.UrlGenerateSign action and are set to 1 when the URL signing key is specified in the Service Rule XML file. If the URL signing key is specified by using the URL Signing page or the **url-signature** command for each SE, the UrlGenerateSign action will find the key by the key-id-owner and key-id-number specified in the Rule.UrlGenerateSign action, and the Rule.Validate action will find the key by the KO (key-id-owner) and KN (key-id-number).

The following rules apply for Rule.Validate and Rule.UrlGenerateSign actions:

- key-id-owner and key-id-number are required attributes for the UrlGenerateSign action
- Only http is supported as the protocol attribute value for Rule.UrlGenerateSign; all other values have no affect.
- Rule.Validate supports http, rtsp, and rtmp as the protocol attribute value.

Following is an example of the Service Rule XML file configured with a symmetric key (also known as shared secret):

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>Cisco</CustomerName>
<ApplyAllTier>yes</ApplyAllTier>
<Rule_Patterns>
    <PatternListGrp id = "grp1">
        <Domain>cds.cisco.com</Domain >
    </PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
    <Rule.UrlGenerateSign matchGroup="grp1" protocol="http" key-id-owner="1"
key-id-number="1" key="cisco123" timeout-in-sec="50" />
    <Rule.Validate matchGroup="grp1" key="cisco123" protocol="all"
error-redirect-url="http://wwwin.cisco.com" />
</Rule_Actions>
</CDSRules>
```

Following is an example of the Service Rule XML file configured with an asymmetric key (also known as public key):

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>Cisco</CustomerName>
<ApplyAllTier>yes</ApplyAllTier>
<Rule_Patterns>
    <PatternListGrp id = "grp1">
        <Domain>cds.cisco.com</Domain >
    </PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
    <Rule.UrlGenerateSign matchGroup="grp1" protocol="http" key-id-owner="1"
key-id-number="1" private-key="http://10.74.61.69/vod/private_key.txt"
symmetric-key="ciscociscociscoc" timeout-in-sec="50" />
    <Rule.Validate matchGroup="grp1" public-key="http://10.74.61.69/vod/public_key.txt"
symmetric-key="ciscociscociscoc" protocol="all"
error-redirect-url="http://wwwin.cisco.com" />
</Rule_Actions>
</CDSRules>
```

## Windows Media Streaming ASX Files with URL Signing

The Windows Media Streaming ASX Files with URL Signing feature uses the Rule.UrlGenerateSign rule action in the Service Rule file.

When the playback URL for a Windows Media Streaming live program has an ASX extension, the Content Abstraction Layer (CAL) returns metadata with an ASX file generated that contains both an HTTP URL and an RTSP URL for playback of the live program. These two URLs should be signed so that subsequent requests to playback the live program can be validated by the SE.

The Rule.UrlGenerateSign Rule.Action provides the ability to internally generate URL signatures using Version 2 of the URL signing script (SHA-1 encryption, protocol removed from beginning of the URL, and domain name not included). When the signed URL is sent back to the client as part of the ASX response, the domain name received from the client is added back in.

### ASX File Request Flow

The request flow is as follows:

1. Client requests an ASX file.
2. A Service Rule XML file is configured for the delivery service that contains the new Rule.Action, Rule.UrlGenerateSign. The Rule.UrlGenerateSign Rule.Action element requires the following attribute values: Key Owner, Key Number, and timeout. If the timeout attribute value is not specified, the default value of 30 seconds is used. The range for the timeout value is from 0 to 50 seconds.
3. If the pattern for Rule.UrlGenerateSign is matched, the URL signature is generated by the SE using Version 2 of the URL signing script and the attribute values specified for the Rule.UrlGenerateSign element.

Internally signed URLs will have IS=1. The IS=0 string is for legacy support with some VDSVDS components that use both internal and external signing mechanisms.

Both the HTTP and RTSP signed URLs are contained in the ASX file. The signed URL that is used is determined by which protocol (HTTP or RTSP) is allowed or disallowed in the Windows Media Streaming configuration.

**Note**

If Windows Media Streaming is disabled, a 500 internal server message is sent to the client. The ASX file is not generated if Windows Media Streaming is disabled.

4. The client receives the ASX file with the signed URL. The player parses the ASX file and sends out the request again with the signed URL. The SE receives the signed URL and validates it. If the validation succeeds, the client is served the content.

The Service Rule XML file has to be created and uploaded through the CDSM GUI, then assign to the delivery service.

### **Rule\_UrlGenerateSign Configuration Example for Two Delivery Services and One Origin Server**

As previously mentioned, the Rule\_UrlGenerateSign rule action works with files that have the .asx extension, which are requests for Windows Media Streaming live content. The .asx request is first handled by the Web Engine, which treats it as a VOD request.

The following example describes how to configure the Service Rule XML file for two delivery services (one live and one VOD) and one Origin server. The two delivery services, wmt-live and wmt-vod, have the same content origin server that has an RFQDN of cds.cisco.com.

Create two Service Rule XML files:

- url\_generate.xml—Assign this Service Rule file to the wmt-vod delivery service
- url\_validate.xml—Assign this Service Rule file to the wmt-live delivery service

When the first request, `http://cds.cisco.co/wmt-live.asx`, comes in, the Rule\_UrlGenerateSign rule in the url\_generate.xml file generates a signed request in the reply. See the [Example of url\\_generate.xml File](#) section. Following is an example of the reply:

```
<ASX version="3">
<Entry>
  <ref HREF="rtsp://cds.cisco.com/wmt-live?
SIGV=3&IS=1&KO=1&KN=1&US=sy1FVrgXxH4=9wWgxPK4fd01b9ShREo4SqkojQAYndseOfn8cQf+5JdtpbRNy0eCS
dQ/ndXbhhYQSBXh3PMq04YG4umA/yDDMeB3TfhHSWQvkaDLLOjJa0xUYQ==" />
  <ref HREF="http://cds.cisco.com/wmt-live?
IGV=3&IS=1&KO=1&KN=1&US=sy1FVrgXxH4=9wWgxPK4fd01b9ShREo4SqkojQAYndseOfn8cQf+5JdtpbRNy0eCSD
Q/ndXbhhYQSBXh3PMq04YG4umA/yDDMeB3TfhHSWQvkaDLLOjJa0xUYQ==" />
</Entry>
</ASX>
```

When the second request comes in:

```
rtsp://cds.cisco.com/wmt-live?=3&IS=1&KO=1&KN=1&US=sy1FVrgXxH4=9wWgxPK4fd01b9ShREo4SqkojQA
YndseOfn8cQf+5JdtpbRNy0eCSDQ/ndXbhhYQSBXh3PMq04YG4umA/yDDMeB3TfhHSWQvkaDLLOjJa0xUYQ==
```

The Rule\_Validate rule in the url\_validate.xml file validates the request. See the [Example of the url\\_validate.xml File](#).

#### **Example of url\_generate.xml File**

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Cisco</CustomerName>
  <ApplyAllTier>yes</ApplyAllTier>
  <Rule_Patterns>
```

```

<PatternListGrp id = "grp1">
    <Domain>cds.cisco.com</Domain >
</PatternListGrp>
</Rule_Patterns>

<Rule_Actions>
    <Rule_UrlGenerateSign matchGroup="grp1" protocol="http" key-id-owner="1"
key-id-number="1" private-key="http://10.74.61.69/vod/private_key.txt"
symmetric-key="ciscociscociscoc" timeout-in-sec="50" />
</Rule_Actions>
</CDSRules>

```

### Example of the url\_validate.xml File

```

<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Cisco</CustomerName>
    <ApplyAllTier>yes</ApplyAllTier>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <Domain>cds.cisco.com</Domain >
        </PatternListGrp>
    </Rule_Patterns>

    <Rule_Actions>
        <Rule_Validate matchGroup="grp1"
public-key="http://10.74.61.69/vod/public_key.txt" symmetric-key="ciscociscociscoc"
protocol="all" error-redirect-url="http://wwwin.cisco.com" />
    </Rule_Actions>
</CDSRules>

```

### Service Rule Action Order for Rule\_Validate and Rule\_UrlGenerateSign

The Rule\_Actions processing is the same as described in “[Rule Action Processing](#)” section on page [E-11](#); all Rule\_Actions are processed in the same order as they are listed in the Rule\_Actions element. However, for Rule\_Validate and Rule\_UrlGenerateSign, if the pattern is matched, and the URL validation or URL generation fails and there is a Rule\_UrlRewrite or Rule\_NoCache listed before, neither will be performed. Because the Rule\_Validate or Rule\_UrlGenerateSign process failed (validation or generation respectively), the authserver returns Action\_Deny and the corresponding rule action (either Action\_validate or Action\_UrlGenerateSign). The Action\_rewrite is not returned, nor is the action for Rule\_NoCache if it is listed. This is true whenever Rule\_Validate or Rule\_UrlGenerateSign is listed, the pattern is matched, and the action fails (either URL validation or URL signing fails).

If either Rule\_Validate or Rule\_UrlGenerateSign is listed, the pattern is matched, and the action is successful, and if Rule\_UrlRewrite is listed, then the Action\_rewrite is returned and so is the Action\_validate and Action\_UrlGenerateSign (if all three rules are listed).

### Service Rule Processing for Rule\_Validate and Rule\_UrlGenerateSign

This section describes the rule processing in general, and specifically addresses when Rule\_UrlGenerateSign and Rule\_Validate are included in the Rule\_Actions.



**Note** Pattern match failure as described in this section means that none of the patternGrps specified as part of the matchGroup matched for a particular action.

**Rule\_Allow**

If pattern match fails, the request is blocked and there is no further processing of the remaining rules.  
If pattern match is successful, rule processing continues to the next rule action.

**Rule\_Block**

If there is a pattern match for Rule\_Block, the request is blocked and there is no further processing of the remaining rules.

If there is no pattern match for Rule\_Block, rule processing continues to the next rule action.

**Rule\_UrlRewrite, Rule\_NoCache, Rule\_Validate, Rule\_UrlGenerateSign—Pattern Match Failure Case**

If pattern match fails, rule processing continues to the next rule action and there is no return value for the specified rule action. For example, if the rule action was Rule\_Validate and the pattern match failed, there would be no URL validation performed on the request.

In the following XML example, because the pattern match failed for the action Rule\_Validate, authserver does not return Action\_validate. Because the Rule\_UrlRewrite and Rule\_UrlGenerateSign pattern matches were successful, authserver returns those actions in its response.

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>ATT</CustomerName>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <UrlRegex>asx</UrlRegex>
        </PatternListGrp>
        <PatternListGrp id = "grp2">
            <UrlRegex>abcd</UrlRegex>
        </PatternListGrp>
    </Rule_Patterns>
    <Rule_Actions>
        <Rule_UrlGenerateSign matchGroup = "grp1" key-id-owner = "1" key-id-number = "1"
timeout-in-sec = "30" protocol = "http" />
        <Rule_Validate matchGroup = "grp2" error-redirect-url="http://4.0.1.6/index.html"
protocol = "http" />
        <Rule_UrlRewrite matchGroup = "grp1" protocol = "http" regsub = "DejaVu"
rewrite-url = "dummy" />
    </Rule_Actions>
</CDSRules>
```

**Rule\_UrlRewrite, Rule\_No\_Cache, Rule\_Validate, Rule\_UrlGenerateSign—Pattern Match Success Case**

If pattern match is successful, the actions are processed as described in the following subsections:

- [Rule\\_Validate, Rule\\_UrlGenerateSign—Validation Fails, Signing Fails, Configuration Failure](#)
- [Rule\\_UrlRewrite and Rule\\_NoCache—Rewrite Fails](#)
- [Rule\\_UrlRewrite, Rule\\_NoCache, Rule\\_Validate, Rule\\_UrlGenerateSign—Success](#)

**Rule\_Validate, Rule\_UrlGenerateSign—Validation Fails, Signing Fails, Configuration Failure**

Rule\_Validate and Rule\_UrlGenerateSign have a higher priority than Rule\_UrlRewrite or Rule\_NoCache. If the pattern matches, but the function fails (URL validation fails, URL signing fails, or there is a configuration failure), there is no further processing of the rule actions and the request is denied.

authserver returns [Action\_Deny + Action\_validate] if validation/UrlSignature generation fails.

authserver returns [Action\_Deny + Action\_UrlGenerateSign] if UrlSignature generation fails.

Also, the value from previous actions is not returned in either case. For example, if Rule\_UrlRewrite preceded Rule\_UrlGenerateSign, and Rule\_UrlRewrite was successful, but Rule\_UrlGenerateSign failed, authserver does not return the value for Action\_Rewrite. Similarly, if Rule\_UrlRewrite preceded Rule\_Validate, and Rule\_UrlRewrite was successful, but Rule\_Validate failed, authserver would not return the value for Action\_Rewrite. The same logic that is described for Rule\_UrlRewrite applies to Rule\_NoCache as well.

The following XML example illustrates the above scenarios:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>ATT</CustomerName>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <UrlRegex>asx</UrlRegex>
        </PatternListGrp>
        <PatternListGrp id = "grp2">
            <UrlRegex>abcd</UrlRegex>
        </PatternListGrp>
    </Rule_Patterns>
    <Rule_Actions>
        <Rule_UrlRewrite matchGroup = "grp1" protocol = "http" regsub = "DejaVu"
        rewrite-url = "dummy" />
        <Rule_UrlGenerateSign matchGroup = "grp1" key-id-owner = "1" key-id-number = "1"
        timeout-in-sec = "30" protocol = "http" />
        <Rule_Validate matchGroup = "grp2" error-redirect-url="http://4.0.1.6/index.html"
        protocol = "http" />
    </Rule_Actions>
</CDSRules>
```

### **Rule\_UrlRewrite and Rule\_NoCache—Rewrite Fails**

Rule\_UrlRewrite and Rule\_NoCache have a lower priority than Rule\_Validate and Rule\_UrlGenerateSign. If the pattern matches, but the Rule\_UrlRewrite or Rule\_NoCache fails, authserver does not return Action\_Deny and processing of remaining rules actions continues. If Rule\_UrlRewrite fails, authserver does not return the value for Action\_Rewrite. If Rule\_NoCache fails, authserver does not return its value.

### **Rule\_UrlRewrite, Rule\_NoCache, Rule\_Validate, Rule\_UrlGenerateSign—Success**

If the Rule\_UrlRewrite action is successful, authserver response contains the Action\_Rewrite and the new rewritten URL is sent. Processing of the remaining rules actions continues.

If the Rule\_NoCache action is successful, authserver sends the instructions to not cache the content. Processing of the remaining rules actions continues.

If Rule\_Validate is successful, authserver response contains the Action\_Validate.

If Rule\_UrlGenerateSign is successful, authserver response contains Action\_UrlGenerateSign.

# Converting Old Windows Media Streaming Service Rules for URL Signing and Validation

This section provides examples of converting the generate-url-signature and validate-url-signature service rule actions for Windows Media Streaming to the Service Rule format.



**Note** All Windows Media Streaming per-device service rules configured for URL signature and validation must be converted to the per-delivery service Service Rule XML file. This change only applies to the generate-url-signature and validate-url-signature service rule actions for Windows Media Streaming. The other service rule actions (allow, block, no-cache, redirect, refresh, replace, and rewrite) still use the per-device service rule configuration for Windows Media Streaming.

## Perform URL Signature Generation on Requests

The following example shows the commands for configuring a service rule that performs URL signature generation on requests from the domain wmtvod.com using the old mechanism:

```
SE (config)# url-signature key-id-owner 1 key-id-number 1 key cisco123
SE (config)# rule enable
SE (config)# rule action generate-url-signature key-id-owner 1 key-id-number 1
pattern-list 1 protocol http
SE (config)# rule pattern-list 1 domain wmtvod.com
```

The Service Rule XML file for the above rule is as follows:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Cisco</CustomerName>
    <ApplyAllTier>yes</ApplyAllTier>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <Domain>wmtvod.com</Domain >
        </PatternListGrp>
    </Rule_Patterns>

    <Rule_Actions>
        <Rule.UrlGenerateSign matchGroup = "grp1" protocol = "http" key="cisco123
key-id-owner="1" key-id-number="2" timeout-in-sec="30"/>
    </Rule_Actions>
</CDSRules>
```

## Perform URL Signature Validation on Requests

The following example shows the commands for configuring a service rule that performs URL signature validation on requests from the domain, wmtvod.com using the old mechanism:

```
SE (config)# rule enable
SE (config)# rule action validate-url-signature error-redirect-url www.cisco.com
pattern-list 1 protocol all
SE (config)# rule pattern-list 1 domain wmtvod.com
```

The Service Rule XML file for the above rule is as follows:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Capricious</CustomerName>
    <Rule_Patterns>
```

## ■ Rule Actions for Flash Media Streaming

```

<PatternListGrp id = "grp1">
    <Domain>wmtvod.com</Domain>
</PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
    <Rule_Validate matchGroup = "grp1" protocol = "all" key="cisco123"
error-redirect-url="http://www.cisco.com"/>
</Rule_Actions>
</CDSRules>

```



**Note** The Rule\_Validate action can also be configured without the *key* attribute, if the key is defined for each SE by using the CDSM GUI URL Signing page or by using the **url-signature** command.

## Rule Actions for Flash Media Streaming

Service rules for Flash Media Streaming are now configured using the Service Rule file. By associating the Service Rule file with a delivery service, all service rules defined in the file are applied to all SEs in the delivery service.

The following service rule actions are supported for Flash Media Streaming:

- Allow (Rule\_Allow)
- Block (Rule\_Block)
- URL signature validation (Rule\_Validate)
- SWF file validation (Rule\_SwfFileValidate)
- DSCP (Rule\_Dscp)



**Note** Starting from Release 3.3, VDS-IS supports per session DSCP marking for Flash Media streaming, VOD, and Live.

## Converting Old Flash Media Streaming Service Rules

The following example shows an example of each rule action for Flash Media Streaming using the old mechanism and the conversion to the Service Rule format.



**Note** Currently, the header field referrer is not supported.

### Block Requests

The following example shows the commands for configuring a service rule that blocks RTMP requests from the domain fmsvod.com using the old mechanism:

```

SE (config)# rule enable
SE (config)# rule action block pattern-list 1 protocol rtmp
SE (config)# rule pattern-list 1 domain fmsvod.com

```

The Service Rule XML file for the above rule is as follows:

```

<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">

```

```

<Revision>1.0</Revision>
<CustomerName>Capricious</CustomerName>
<Rule_Patterns>
    <PatternListGrp id = "grp1">
        <Domain>fmsvod.com</Domain>
    </PatternListGrp>
</Rule_Patterns>

<Rule_Actions>
    <Rule_Block matchGroup = "grp1" protocol = "rtmp" />
</Rule_Actions>
</CDSRules>

```

### Allow Requests

The following example shows the commands for configuring a service rule that allows RTMP requests from the domain fmsvod.com using the old mechanism:

```

SE (config)# rule enable
SE (config)# rule action allow pattern-list 1 protocol rtmp
SE (config)# rule pattern-list 1 domain fmsvod.com

```

The Service Rule XML file for the above rule is as follows:

```

<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Capricious</CustomerName>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <Domain>fmsvod.com</Domain>
        </PatternListGrp>
    </Rule_Patterns>

    <Rule_Actions>
        <Rule_Allow matchGroup = "grp1" protocol = "rtmp" />
    </Rule_Actions>
</CDSRules>

```

### Perform URL Signature Validation on Requests

The following example shows the commands for configuring a service rule that performs URL signature validation on requests from the domain fmsvod.com using the old mechanism:

```

SE (config)# rule enable
SE (config)# rule action validate-url-signature error-redirect-url www.cisco.com
pattern-list 1 protocol rtmp
SE (config)# rule pattern-list 1 domain fmsvod.com

```

The Service Rule XML file for the above rule is as follows:

```

<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Capricious</CustomerName>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <Domain>fmsvod.com</Domain>
        </PatternListGrp>
    </Rule_Patterns>

    <Rule_Actions>
        <Rule_Validate matchGroup = "grp1" protocol = "rtmp"
        error-redirect-url="http://www.cisco.com"/>
    </Rule_Actions>
</CDSRules>

```

## ■ Rule Actions for Flash Media Streaming

```
</CDSRules>
```

### Match on Regular Expression

Pattern matching can be performed on a regular expression instead of matching on the domain name in any of the Flash Media Streaming service rules. The following example shows the commands for configuring a service rule that allows RTMP requests that match the string “clouds” using the old mechanism:

```
SE (config)# rule enable
SE (config)# rule action allow pattern-list 1 protocol rtmp
SE (config)# rule pattern-list 1 url-regex clouds
```

The Service Rule XML file for the above rule is as follows:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Capricious</CustomerName>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <UrlRegex>clouds</UrlRegex>
        </PatternListGrp>
    </Rule_Patterns>

    <Rule_Actions>
        <Rule_Allow matchGroup = "grp1" protocol = "rtmp" />
    </Rule_Actions>
</CDSRules>
```

### Match on Source IP address

Pattern matching can be performed on the source IP address instead of matching on the domain name in any of the Flash Media Streaming rules. The following example shows the commands for configuring a service rule that allows RTMP requests that match the source IP address 209.165.201.1 using the old mechanism:

```
SE (config)# rule enable
SE (config)# rule action allow pattern-list 1 protocol rtmp
SE (config)# rule pattern-list 1 src-ip 209.165.201.10 255.255.0.0
```

The Service Rule XML file for the above rule is as follows:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Capricious</CustomerName>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <SrcIp>209.165.201.10/16</SrcIp>
        </PatternListGrp>
    </Rule_Patterns>

    <Rule_Actions>
        <Rule_Allow matchGroup = "grp1" protocol = "rtmp" />
    </Rule_Actions>
</CDSRules>
```

## Support for SWF Validation

Small Web Format (SWF) file validation is supported by using the Service Rule XML file. A client player generates the signature for an SWF file and the signature is sent to the Flash Media Streaming engine. The client SWF file is validated against the SWF file on the SE. If the subscriber edits the SWF file or uses a malicious SWF file, the signatures differ and the request is rejected.

### SWF Validation Process

If SWF validation is required, the Authorization Server tells Flash Media Streaming whether SWF file validation needs to be performed or not for a particular delivery service. Flash Media Streaming then fetches and accesses the SWF file and uses it to validate the request.

The Authorization Server determines if the SWF file verification needs to be done or not based on the rules listed in Service Rule file.


**Note**


---

The SWF file must be stored on the local disk of the SE. In a cache-miss case, the entire SWF file must be retrieved before SWF validation can continue.

---

An algorithm is used to generate a hash of the SWF file by using the file size of the original SWF file and the location.

If the Authorization Server says SWF verification is not required, a property is set telling Flash Media Streaming to bypass it.

The SWF validation is performed by comparing the hash generated by Flash Media Streaming with the hash sent by the client. The client-side hash is generated automatically by the Flash Media player when an RTMP connection is made.

If the hashes match, the SWF validation is successful and the request is allowed; if the hashes do not match, the SWF validation is not successful and the request is denied.


**Note**


---

The SWF validation does not apply to interactive applications.

---

Web Engine revalidation should be enabled so that the latest SWF file is used. If Web Engine revalidation is not enabled, then an older SWF file may be used for validation for up to one hour after the entry in the cache of hashes has expired. Revalidation is enabled by default on the Web Engine.

If Authorization Server is disabled, SWF validation is always performed.

---

### Interaction with Web Engine

When Web Engine receives a Flash Media Streaming request and SWF validation is enabled for the delivery service, the original SWF file must be on the local disk. If the file is not found in the /local/local1/swfs directory, Web Engine performs a lookup and the file is cached on the local disk. If the SWF file is found at the cached location, Web Engine performs a cache revalidation, if applicable. In a cache-miss case, the entire SWF file must be retrieved before SWF validation can continue. If the URL of the SWF file is an Origin Server fully-qualified domain name (OFQDN)-based URL or a Service Router fully-qualified domain name (RFQDN)-based URL, Web Engine caches the file to the local disk. If the URL is other than these two, Web Engine treats it as a proxy request and the Flash Media Streaming engine writes the file to disk at the /local/local1/swfs directory (the file is deleted after the request is processed).

There are five possible successful responses from Web Engine: cache miss, cache hit, alien hit, pre-position, or proxy. In the first four cases, Flash Media Streaming reads the SWF file directly and adds it to the cache of hashes. In the proxy request case, the file is written to the /local/local1/swfs directory and deleted after the SWF validation is complete. The hash is not added to the cache of hashes in the proxy-request case.



- Note** If the SWF file is uploaded to individual SEs at the /local/local1/swfs directory, revalidation of the SWF file is not performed, which means that if the SWF file is modified, the new file has to be uploaded to the SEs again. This has to be done for every SE in the delivery service.

If Authorization Server is disabled, or if the SWF validation is not enabled, the SWF validation is also not performed on the locally uploaded files. The SWF Validation feature assumes that the SWF file is being requested from an HTTP location; therefore, if the SWF file is located on a personal computer with a path similar to "c:/Documents/," the SWF validation rejects the request.

## Service Rule File Example for SWF Validation

Following is an example of the SWF validation in the Service Rule XML file:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Company</CustomerName>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <Domain>demo.cdsis.com</Domain>
        </PatternListGrp>
    </Rule_Patterns>
    <Rule_Actions>
        <Rule_SwfFileValidate matchGroup = "grp1" protocol = "rtmp" />
    </Rule_Actions>
</CDSRules>
```

The *matchGroup* attribute value is the list of PatternListGrp *id* attributes. The *protocol* attribute value must be rtmp, rtmpf, rtmpm, or all.



- Note** Multiple protocols can be specified for the same rule by including each protocol as a value of the *protocol* attribute in the form of a comma-separated string.

Whether a Rule\_SwfFileValidate is matched or not, rule processing continues to the next configured rule. Rule\_SwfFileValidate action enables Flash Media Streaming to perform SWF file validation. If the Rule\_SwfFileValidate pattern is matched and the SWF file validation fails, then the request is rejected.

## Support for DSCP Marking

The DSCP per delivery service requires to configure domain name in the rule file. The rule will match the *matchGroup* defined by a regex pattern or domain name and the attribute *dscp-bits* will be applied to the matching pattern. The attribute is the DSCP value ranging from 0 to 63. Absence of the tag in the rules xml file shall assume default DSCP value to 0.

## Service Rule File Example for DSCP Marking

The following example shows the commands for configuring a service rule that allows RTMP requests that match the amsvod domain name using the old mechanism:

```
SE (config)# rule enable
SE (config)# rule action allow pattern-list 1 protocol rtmp
SE (config)# rule pattern-list 1 domain amsvod
```

The Service Rule XML file for the above rule is as follows:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>BT</CustomerName>
<Rule_Patterns>
<PatternListGrp id = "grp1">
<Domain>amsvod.com</Domain>
</PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
<Rule_Dscp matchGroup = "grp1" protocol = "all" dscp-bits = "20" />
</Rule_Actions>
</CDSRules>
```

# Service Rule File Example

The following is an example of a Service Rule file:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>Capricious</CustomerName>
<Rule_Patterns>
<PatternListGrp id = "grp1">
<UrlRegex>videos</UrlRegex>
<Domain>rfqdn.cds.com</Domain>
</PatternListGrp>
<PatternListGrp id = "grp2">
<Domain>dummy.cds.com</Domain>
<SrcIp>10.10.10.10</SrcIp>
</PatternListGrp>
<PatternListGrp id = "grp3">
<SrcIp>10.21.148.231</SrcIp>
</PatternListGrp>
<PatternListGrp id = "grp5">
<UrlRegex>/*</UrlRegex>
</PatternListGrp>
<PatternListGrp id = "grp6">
<Domain>rfqdn.cds.com</Domain>
</PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
<Rule_Allow matchGroup = "grp1,grp5" protocol = "http" />
<Rule_UrlRewrite matchGroup = "grp1" protocol = "http" regsub = "videos"
rewrite-url = "http://dummy.cds.com" />
<Rule_Block matchGroup = "grp3" protocol = "http" />
<Rule_Validate matchGroup = "grp5" protocol = "http" error-redirect-url =
"http://wwwin.cisco.com" exclude-validation = "all" />
</Rule_Actions>
```

## ■ Service Rule File Example

```
</CDSRules>
```

# Service Rule File for URL Validation and the Exclude-Validation Attribute

As part of the URL Signing feature, to validate signed URLs for the Web Engine, you must configure the Service Rule file for URL Validation. The exclude-validation attribute offers the option to exclude the client IP address , the expiry time, or both from the URL validation process. The following sections explain the different exclude validation options:

- [Exclude Client IP address from URL Validation](#)
- [Exclude Expiry Time from URL Validation](#)
- [Exclude Both the Client IP address and the Expiry Time from URL Validation](#)

## Exclude Client IP address from URL Validation

While performing URL validation, the SE compares the IP address from which it received the request and the CIP field in the signed URL request. The client IP address is a required parameter and is displayed as the CIP field in the signed URL request. If you configure the exclude-validation attribute with the client-ip value in the Service Rule XML file, the URL validation process ignores the client IP address during the validation process.

Following is an example of the Service Rule XML file with the exclude-validation attribute set to client-ip:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>ATT</CustomerName>
<Rule_Patterns>
  <PatternListGrp id = "grp1">
    <Domain>iphone.com</Domain>
  </PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
  <Rule_Validate matchGroup = "grp1" protocol="http" exclude-validation="client-ip"
error-redirect-url = "http://wwwin.cisco.com"/>
</Rule_Actions>
</CDSRules>
```

## Exclude Expiry Time from URL Validation

Without the exclude-validation expiry-time attribute, he generated URL would be valid only for a stipulated period of time mentioned at the time of signing. This is indicated in the ET field in the signed URL. The ET field value is generated with respect to the local time on the server used for signing. The expiry time relies on the synchronization of the devices; for more information, see the [“Importance of Device Synchronization” section on page H-13](#).

On receiving the request, the URL validation process compares the time stamp on the SE with the time stamp in the ET field of the received request. If the time stamp on the request is less than the time stamp on the SE, the request is rejected because of the expiry time lapse.

To bypass the expiry time validation, use the exclude-validation attribute with the expiry-time value in the Service Rule XML file.

Following is an example of the Service Rule XML file with the exclude-validation attribute set to expiry-time:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>ATT</CustomerName>
<Rule_Patterns>
<PatternListGrp id = "grp1">
<Domain>iphone.com</Domain>
</PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
<Rule_Validate matchGroup = "grp1" protocol="http" exclude-validation="expiry-time"
error-redirect-url = "http://wwwin.cisco.com"/>
</Rule_Actions>
</CDSRules>
```

## Exclude Both the Client IP address and the Expiry Time from URL Validation

The exclude-validation attribute with the all value excludes both the client-ip and the expiry-time from the URL validation process. Meaning the SE considers the request successful even if the request comes from a different client than what is mentioned in the signed URL and the expiry-time has lapsed.

Following is an example of the Service Rule XML file with the exclude-validation attribute set to all:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>ATT</CustomerName>
<Rule_Patterns>
<PatternListGrp id = "grp1">
<Domain>iphone.com</Domain>
</PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
<Rule_Validate matchGroup = "grp1" protocol="http" exclude-validation="all" error-redirect-url = "http://wwwin.cisco.com"/>
</Rule_Actions>
</CDSRules>
```



**Note** The *exclude-validation exclude-domain* attribute instructs the SEs to ignore the domain in the URL when processing the validation of the signed URL.

**■ Service Rule File Example**



# ABR Session-Based Encryption and Session Tracking

This appendix describes ABR Session-Based Encryption and Session Tracking. This appendix consists of the following topics:

- [Introduction, page F-1](#)
- [Configuring Session-Based Encryption and Session Tracking, page F-5](#)

## Introduction

Session-Based Encryption and Session Tracking is provided for Apple HTTP Live Streaming (HLS) and Microsoft HTTP Smooth Streaming (HSS) Adaptive Bit Rate (ABR) protocols. Current content workflows may require content have digital rights management (DRM) and encryption applied prior to being sent to authoritative storage or CDN delivery, and often multiple formats and DRM schemes must be supported by the service provider, which results in high storage capacity requirements both within the authoritative store as well as the Videoscape Distribution Suite, Internet Streamer (VDS-IS) cache hierarchy. Session-Based Encryption at the edge can dramatically reduce the overall storage requirements.

The Session-Based Encryption and Session tracking (SBE) feature introduces the *Session Construct* term to create the concept of session within the VDS-IS, even though HTTP ABR is inherently sessionless. The uses of the Session Construct are threefold:

- Session Tracking— Useful for reporting, billing, and troubleshooting purposes. The Session Construct allows the VDS-IS to mark transaction log entries for the many individual ABR fragment requests with a common parameter for correlation to the broader user session between the user and the service provider CDN.
- Access Protection—Through the use of optionally signed cookies that have expiration times or URL query strings, along with the Session Construct, only the intended clients (IP address validation) may successfully request content from the VDS-IS.
- Session-Based Encryption—Ensures that the VDS-IS can encrypt with the correct key for the specific client session. The Session Construct is fundamental to the implementation of session-based encryption.



### Note

SBE is supported per user device and per content request. So, if a user has two HLS content requests from the same device for the same content, there are two separate sessions that are tracked and each has its own key.

Session-based encryption supports encryption key message (creation, request, rotation, and deletion) communication over HTTP and HTTPS with an external key management server (KMS).

The ABR Session Tracking and Session-Based Encryption feature for HLS and HSS protocols addresses the following requirements:

- Support ABR session tracking across multiple TCP sessions and content access protection using HTTP cookies.
- Session tracking across bitrate shifts.
- Support SBE for HLS as per the Apple HTTP Live Streaming specification.
- Function irrespective of the underlying storage mechanism (for example, NAS, prefetched content, and cached content).
- Support out-of-band manifest use-case for HLS and HSS, where the manifest handling is done outside the SE and the SE receives only the video segment or fragment requests
- Support HSS with out-of-band manifests, and with whole fragment encryption (non-PIFF)
- Supports configurable HSS encryption key messages (create, request, rotation, delete) to different KMSs
- Supports periodic key rotation for HLS
- Support media session resiliency across SE failover

In Release 3.2, VDS-IS supports Generic Session Tracking and Logging. Generic Session Tracking is used to track the HTTP user session based on session id which is a unique id during the entire session life circle.

This tracking is not ABR protocol specific, the mechanism is generic. All the session information elements can be retrieved from incoming request URL (Intercept URL) and cookie. New and existing SBE rules are configured to retrieve this kind of session information. The requests that cannot be tracked will still be served. Generic Session Tracking does not support Session based encryption.



**Note** If both Generic Session and ABR Session tracking are enabled in CDSM GUI, the Generic session tracking will get the priority and track the session.

## HLS Session-Based Encryption

Session-based-encryption encrypts HLS video content with a unique key per device and content. The key consists of AES-128 CBC cipher for encryption and decryption. The EXT-X-KEY tag in the m3u8 playlist file is used by clients to retrieve the key and decrypt the content.



**Note** For HLS live Delivery Service with encryption, when the rate of clients joining is about 300 clients per seconds, it is possible for the clients to get redirected to the Origin server because the SE memory usage threshold is exceeded. To prevent clients getting redirected to the Origin server under these conditions, follow these steps:

- Make sure the HLS manifest file (m3u8 playlist) has the cache-control max-age header enabled in the Origin server.
- Make sure the transport-stream segment files have the cache-control header disabled in the Origin server.

## HLS Solution Components

A typical media distribution and delivery systems has the following components:

- Encapsulator—Responsible for packaging the content into MPEG2-TS segments and creating the m3u8 playlist files.
- Authorization/Authentication Server—Responsible for user authentication and media entitlement. Typically this consists of a URL signature with identifiers (user, device, media, session) or an authentication token that may need to be validated by the SE, and the URL for the manifest (m3u8 playlist) file.
- Key Management Server (KMS)—Creates and provides keys used for encryption or decryption to the streaming SE.
- SE—Provides edge caching and streams content to the client. When session-based-encryption is enabled, the content is encrypted here. The edge SE interacts with the KMS to retrieve the encryption keys, and updates the manifest file with the key URI that is provided to the client.
- Client—Downloads the playlist and segments, retrieves the key URI, and decrypts the segments for playing the content.

## HLS Out of Band Manifests

In systems where there is a separate manifest generator or session ID generator, the SE receives only the video segment requests. In such cases, the session is created on the first video segment request and session encryption is performed identical to the case where the SE received the manifest request. Session tracking is performed based on the URL query string, which typically has a session ID generated by the manifest generator. We do not recommend using a cookie-based session tracking with out-of-band manifest.

## HSS Session-Based Encryption

Session-based encryption for HSS supports the following:

- Out-of-band manifests (only)
- Whole fragment encryption
- Caching only the small fragments for both VOD and live streaming
- AES-128 CBC cipher for encryption and decryption
- One key per session (no key rotation)

With out-of-band manifest for HSS, the IIS Smooth Streaming Client Manifest (ISM) file (also known as the client manifest file) and the key URI are sent to the Windows Silverlight client by the manifest generator. The SE only receives the fragment requests from the client; not the client manifest file. After the SE receives the client manifest file, it gets the key from the KMS, encrypts the video fragments, and sends them to the client.

The same statistics counters used for HLS are also used for HSS.



**Note** Protected Interoperable File Format (PIFF) encryption is not currently supported.

## Session Tracking

For session tracking, both external and internal session IDs are supported. External session IDs are provided by the entitlement server, DRM system, or manifest generator, and are delivered to the VDS-IS in the client request. In other scenarios, the session ID is generated by a session state manager and delivered to the VDS-IS as part of the publish-URL. The session ID is stored in the session cookie. When the client downloads the ABR manifest file at the start of content delivery, the SE sends a cookie along with the manifest file response to the client. The cookie is sent back to the SE in all subsequent manifest and video fragment requests. If an external session ID is not received, an internal session ID is created by the VDS-IS for internal purposes.

### Session Cookie

The session cookie includes session information (session ID, key parameters, expiry, and MD5 hash of cookie), and expires, path, and domain control of the cookie. When the SessionSinfoTimeout is configured in the Service Rule XML file for the Delivery Service, an expiry time stamp is added to the cookie. If the SessionSinfoTimeout is reached, then the client requests are considered invalid. For this mechanism to be effective for content access protection, the SessionSinfoTimeout is set for a few minutes and refreshed periodically. The cookie expiry is refreshed when a manifest or fragment request comes in after 50 percent of the SessionSinfoTimeout has elapsed but has not expired. Following is an example of a session cookie:

```
Cookie:sinfo=sid=6a8-I-617F442F03277469C5BC073265493BACC129~et=1354357286~pt=/sample/~~md5=E6C36B0E98B4F42E993E9C10B1BF75EE
```

### ABR Session Tracking Client IP address Validation

When the SessionClientIpCheckEnable parameter in the Service Rule XML file is set to enable, the SE validates the client IP address for each fragment request in the following cases:

- Client always resides behind a managed client, and the client IP address known to the SE does not change during the playout session.
- For URL query string, a unique manifest file is generated for each client and the client IP address is sent in each fragment request URL. For session cookie, there is no need for a unique manifest, unless the encryption requires it.

### Generic Session Tracking Client IP address Validation

Generic session tracking uses cookie to validate the client IP address.

- The SessionCookieTrackingEnable parameter should be enabled together with the SessionClientIpCheckEnable parameter.
- Content Access protect for Client IP address validation—if the client request is in content access protect scope, the request will be rejected if client ip validation failed.

#### A Special Use Case:

- URL query tracking and cookie tracking mode—The query string exists in the first client request that triggers the session. The first client request contains the cookie from the first response. The Session's client IP address comes from Client IP field in the first request's query string instead of its socket IP address.

## Key Parameters

The key parameters consist of the following variables:

- Key Content-ID—Four-byte number that identifies a user session to the KMS. Content ID is not related to session tracking, but is used as an alternative to the session ID when interfacing with the KMS. Some KMSs only accept a 4-byte session ID, while others use a full session iD (external or internal).
- Key Rotation—Variables stored in the session cookie are used to calculate the key rotation, such that even if an SE failover or configuration change occurs during a session, the correct key is retrieved from the KMS for encryption.

# Configuring Session-Based Encryption and Session Tracking

The Service Rule file provides configuration settings for Session-Based Encryption and Session Tracking.

To enable session tracking for a Delivery Service, the following must be enabled:

- **Enable Generic Session Tracking**—Enables Generic session tracking at all locations
- **Enable HSS Session Tracking**—Enables HSS session tracking at all locations
- **Enable HLS Session Tracking**—Enables HLS session tracking at all locations

See the “[Creating Delivery Service](#)” section on page 5-16, for more information.

The transaction logs and Session Log must be enabled on each SE participating in session logging. For more information, see the “[Configuring Transaction Logs](#)” section on page 4-30.



**Note** It is recommended to disable session tracking and also, remove the Service Rule file from the Delivery Service for a better performance.

## Service Rule Configuration for Session-Based Encryption and Session Tracking

The Rule\_SetAction action is a Rule\_Actions subelement in the Service Rules schema file (CDSRules.xsd). For more information about the Service Rules, see [Appendix E, “Creating Service Rule Files.”](#) The Rule\_SetAction subelement is used to specify the configuration parameters for Session-Based Encryption.

[Table F-1](#) describes the attributes and subelements of the Rule\_Actions subelement.

**Table F-1 Rule\_SetAction Subelements and Attributes**

Subelements	Attributes	Description
SetParameter	name value	Configuration parameter and value for session-based encryption.
SetRewrite	name regsub rewrite-url	Used to rewrite and set parameters at the same time in one rule. <b>Note</b> Not supported in Release 3.1.

**Table F-1 Rule\_SetAction Subelements and Attributes (continued)**

Subelements	Attributes	Description
SetExecute	moduleType modulePath moduleName moduleMethod	Provides a mechanism to call out a python script from within the rules.  <b>Note</b> Not supported in Release 3.1.
-	name	Name of the Rule_SetAction. In Release 3.1, the value of the <i>name</i> attribute is always Rule_DSConfig.
-	matchGroup	The <i>matchGroup</i> attribute value is the list of PatternListGrp <i>id</i> attributes.
-	protocol	The <i>protocol</i> attribute value is always http.

## Service Rule Example for Session-Based Encryption and Session Tracking

Following is an example of the Service Rule file configured for Session-Based Encryption and Session Tracking. The subelements and attributes are described in [Table F-1](#) and the SetParameter attributes are described in [Table F-2](#).

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>Demo</CustomerName>
<ApplyAllTier>yes</ApplyAllTier>
    <Rule_Patterns>
        <PatternListGrp id = "grp1">
            <Domain>test2.com</Domain>
        </PatternListGrp>
        <PatternListGrp id = "grp2">
            <Domain>test1.com</Domain>
        </PatternListGrp>
        <PatternListGrp id = "grp3">
            <Domain>172.22.96.179</Domain>
        </PatternListGrp>
        <PatternListGrp id = "grp4">
            <Domain>172.22.67.249</Domain>
        </PatternListGrp>
    </Rule_Patterns>
    <Rule_Actions>
        <Rule_Allow matchGroup="grp1,grp2,grp3,grp4" protocol="http"/>
        <Rule_SetAction name="Rule_DSConfig" matchGroup="grp1,grp2,grp3,grp4"
protocol="http">
            <SetParameter name="StreamerSecretKey" value="1A2B3C4a5b6c7d8e9900A1B2C3D4E5F6"/>
            <SetParameter name="ClientCookieTimeout" value="0"/>
            <SetParameter name="SessionClientIpCheckEnable" value="0"/>
            <SetParameter name="SessionCookieTrackingEnable" value="1"/>
            <SetParameter name="SessionIdleTimeout" value="240"/>
            <SetParameter name="SessionSInfoTimeout" value="120"/>
            <SetParameter name="SessionResolveRule#1" value="sessionid=(.*)_sid=$1 "/>
            <SetParameter name="SessionResolveRule#4" value="m3u8:none"/>
            <SetParameter name="SessionResolveRule#2" value="ism:none"/>
            <SetParameter name="SessionResolveRule#3"
value="sessionid=(.*)&clientip=(.*)_sid=$1~cip=$2 "/>
            <SetParameter name="KeyProfileIdleTimeout" value="600"/>
            <SetParameter name="HLSEncryptionEnable" value="0"/>
            <SetParameter name="HSSEncryptionEnable" value="0"/>

```

```

<SetParameter name="HLSInitializationVector"
value="00000000000000000000000000000032"/>
<SetParameter name="HSSInitializationVector"
value="00000000000000000000000000000032"/>
<SetParameter name="HLSKeyRotationFragmentInterval" value="0"/>
<SetParameter name="HLSMaxKeysPerSession" value="1"/>
<SetParameter name="HLSKeyAcquisitionProfile" value="AlphaKMS"/>
<SetParameter name="HSSKeyAcquisitionProfile" value="AlphaKMS"/>
<SetParameter name="KeyProfile#1" value="AlphaKMS"/>
<SetParameter name="AlphaKMS#Request" value="GET,
https://171.70.172.230:4043/cgi-bin/keygen?r=&lt;SESSION-ID&gt;&amp;t=VOD&amp;p=&lt;REKEY-INDEX&gt;"/>
<SetParameter name="AlphaKMS#Delete" value="DELETE,
https://171.70.172.230:4043/cgi-bin/keygen?r=&lt;SESSION-ID&gt;&amp;t=VOD"/>
<SetParameter name="AlphaKMS#LocalKeyURI"
value="https://171.70.172.230:4043/cgi-bin/keygen?r=&lt;SESSION-ID&gt;&amp;t=VOD&amp;p=&lt;REKEY-INDEX&gt;"/>
<SetParameter name="SessionNotificationFormat#1" value="vc-start-stop-msg-1,
POST, &lt;SessionNotif&gt; &lt;br&gt; &lt;SessionId&gt; %SESSION-ID% &lt;/SessionID&gt;
&lt;br&gt; &lt;ClientIP&gt; %CLIENT-IP% &lt;/ClientIP&gt; &lt;br&gt; &lt;/SessionNotif&gt;
&lt;br&gt; "/>
<SetParameter name="SessionNotificationFormat#2" value="vc-start-stop-msg-2,
POST" />
<SetParameter name="SessionStartNotification#1"
value="vc-start-stop-msg-1,http://naveenpk.cisco.com:6666/cgi-bin/ssm"/>
<SetParameter name="SessionStopNotification#1"
value="vc-start-stop-msg-1,http://naveenpk.cisco.com:6666/cgi-bin/ssm"/>
<SetParameter name="SessionStartNotification#2"
value="vc-start-stop-msg-2,http://naveenpk.cisco.com:6666/cgi-bin/ssm?sessionid=%SESSION-I
D&amp;ipaddress=%CLIENT-IP%"/>
<SetParameter name="SessionStopNotification#2"
value="vc-start-stop-msg-2,http://naveenpk.cisco.com:6666/cgi-bin/ssm?sessionid=%SESSION-I
D&amp;ipaddress=%CLIENT-IP%&url=%LAST-REQ-URL%"/> </Rule_SetAction>
</Rule_Actions>
</CDSRules>
```

Following is an example of the Service Rule file configured for Generic Session Tracking and Logging. The subelements and attributes are described in [Table F-1](#) and the SetParameter attributes are described in [Table F-2](#).

```

<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
<Revision>1.0</Revision>
<CustomerName>HLSAT</CustomerName>
<ApplyAllTier>yes</ApplyAllTier>
<Rule_Patterns>
<PatternListGrp id = "grp1">
<Domain>hls.abr.com</Domain>
</PatternListGrp>
</Rule_Patterns>
<Rule_Actions>
<Rule_Allow matchGroup="grp1" protocol="http"/>
<Rule_SetAction name="Rule_DSConfig" matchGroup="grp1" protocol="http">
<SetParameter name="SessionResolveRule#1" value="m3u8:none"/>
<SetParameter name="GenericSessionPlay#1" value="ts:none"/>
<SetParameter name="SessionProtocol#1" value=".*:protocol=$generic_hls"/>
<SetParameter name="SessionBitrate#1" value="sample/(.*):bitrate=$1"/>
<SetParameter name="SessionProfile#1" value="sample/(.*):profile=$1"/>
<SetParameter name="SessionInactivityTimeout" value="6"/>
<SetParameter name="StreamerSecretKey" value="1A2B3C4a5b6c7d8e9900A1B2C3D4E5C8"/>
<SetParameter name="SessionClientIpCheckEnable" value="0"/>
<SetParameter name="SessionIdleTimeout" value="60"/>
<SetParameter name="SessionSinfoTimeout" value="30"/>
<SetParameter name="ClientCookieTimeout" value="31"/>
```

## Configuring Session-Based Encryption and Session Tracking

```

<SetParameter name="SessionStartNotification#1" value="vc-start-stop-msg,
http://10.0.0.12/webtest.htm"/>
<SetParameter name="SessionStopNotification#1" value="vc-start-stop-msg,
http://10.0.0.12/webtest.htm"/>
<SetParameter name="SessionNotificationFormat#1" value="vc-start-stop-msg, GET,
<br>&lt;SessionNotif&gt; &lt;br&gt; &lt;SessionId&gt; %SESSION-ID% &lt;/SessionID&gt;
&lt;br&gt; &lt;FlowId&gt; %FLOW-ID% &lt;/FlowId&gt; &lt;br&gt; &lt;/SessionNotif&gt;
&lt;br&gt;"/>
<SetParameter name="SessionCookieTrackingEnable" value="1"/>
</Rule_SetAction>
</Rule_Actions>
</CDSRules>

```

## SetParameter Names and Values

Table F-2 describes the names and values for the SetParameter subelement.

**Table F-2 SetParameter Name and Values for Session tracking and Session-Based Encryption**

Name	Value
StreamerSecretKey	A 16-byte hexadecimal string that is the secret key shared by all SEs in the Delivery Service. This key is used to generate and validate the session cookie MD5 hash. Following is an example of this parameter:  <SetParameter name="StreamerSecretKey" value="1A2B3C4a5b6c7d8e9900A1B2C3D4E5F6" />  If this parameter is not configured, the default key is NULL.
SessionCookieTrackingEnable	Enables or disables cookie-based session tracking. A value of 1 means enabled. A value of 0 (zero) means disabled. The default is enabled.  When disabled, cookie-related configuration parameters become ineffective.
SessionClientIpCheckEnable	Enables or disables client IP address validation for ABR fragment. A value of 1 means enabled. A value of 0 (zero) means disabled. The default is disabled.  Client IP address validation should be enabled for the following cases: <ul style="list-style-type: none"> <li>The client always resides behind a managed client, and the client IP address known to the SE does not change during the playout session.</li> <li>A unique manifest file is generated for each client and the client IP address is sent in each fragment URL.</li> </ul> The client IP address is cached on the SE in the session object at the start of the session. By default, the SE gets the client IP address from the transport and caches it. However, if there is a client IP address in the incoming URL and a Session Resolve rule to extract the same, then the SE caches this client IP address.  Subsequently, the client IP address is validated by the SE for each fragment request against the client IP address cached in the session object. The SE extracts the client IP address from the transport of the fragment request in order to validate.  <b>Note</b> If client IP address can change during a media session because of NAT or Wifi/3G access change, the client IP address validation should be turned off.  Following is an example of the this parameter:  <SetParameter name="SessionClientIpCheckEnable" value="1" />

**Table F-2 SetParameter Name and Values for Session tracking and Session-Based Encryption (continued)**

Name	Value
SessionIdleTimeout	<p>If there are no HTTP transactions for manifests or fragments for a session, it is considered inactive. If a session is inactive for more than the SessionIdleTimeout, then resources are cleaned up on the SE.</p> <p>A random jitter between 0 and 100 seconds is added to the configured SessionIdleTimeout. This is to reduce the load on the SE by throttling the number of sessions that are cleaned up at a given time. The actual inactivity timeout value is the following:</p> $(\text{Configured Timeout} + 100 \text{ seconds}) \geq \text{Actual Timeout} \geq \text{Configured Timeout}$ <p>The range is from 30 to 7200 seconds. The default is 180 seconds. Following is an example of this parameter:</p> <pre>&lt;SetParameter name="SessionIdleTimeout" value="600" /&gt;</pre> <p><b>Note</b> The SessionIdleTimeout must always be greater than the SessionSinfoTimeout.</p>
SessionInactivityTimeout	<p>The timeout for Session Inactivity (seconds). If no activity till timeout a Session Stop event will be triggered. The value must be always less than existing rule SessionIdleTimeout.</p> <p>If the value is 0, there will be no Session Stop event. The range is from 0 to SessionIdleTimeout-1 seconds. The default is 10 seconds.</p> <p>Following is an example of this parameter:</p> <pre>&lt;SetParameter name="SessionInactivityTimeout" value="10" /&gt;</pre>
SessionSinfoTimeout	<p>Time elapsed since session creation, after which the session cookie expires on the SE, unless refreshed. The SessionSinfoTimeout is used for content access protection from unauthorized users. Any request for a manifest or fragment beyond expiration interval is rejected by the SE.</p> <p>The range is from 30 to 6000 seconds. The default is 300 seconds. Following is an example of this parameter:</p> <pre>&lt;SetParameter name="SessionSinfoTimeout" value="120" /&gt;</pre> <p><b>Note</b> The SessionSinfoTimeout must always be less than the SessionInactivityTimeout.</p>

**Table F-2 SetParameter Name and Values for Session tracking and Session-Based Encryption (continued)**

Name	Value
ClientCookieTimeout	<p>Time elapsed since session creation, after which a session cookie expires on the client. The ClientCookieTimeout is used to set the "expires" control attribute for the media session cookie. This helps in clearing the session cookies on the client, especially for managed clients. However, the SE, which sets the cookie expiry-time for the client, has no control over the unmanaged client clock. So, there is a risk of the cookie getting cleared prematurely, affecting the media playout. Hence, this configuration should be used judiciously. This configuration has no relationship with the SessionSinfoTimeout, which is used by the SE for content access protection.</p> <p>The range is from 0 to 86400 seconds. A value of 0 (zero) means the session expiration is disabled. The default is 0 (zero). Following is an example of this parameter:</p> <pre>&lt;SetParameter name="ClientCookieTimeout" value="0" /&gt;</pre> <p><b>Note</b> If enabled (having a value greater than 0), the ClientCookieTimeout must always be greater than the SessionSinfoTimeout. To ensure that it is greater than the SessionSinfoTimeout, it is mandatory to explicitly specify the SessionSinfoTimeout.</p> <p><b>Note</b> Requires the client clock be synchronized by using NTP.</p>
HLSEncryptionEnable HSSEncryptionEnable	<p>Enables or disables HLS or HSS session-based-encryption feature on SE. A value of 1 means enabled. A value of 0 (zero) means disabled. The default is disabled. Following are examples of these parameters:</p> <pre>&lt;SetParameter name="HLSEncryptionEnable" value="1" /&gt; &lt;SetParameter name="HSSEncryptionEnable" value="1" /&gt;</pre> <p><b>Note</b> When HLS encryption is enabled, the HLSInitializationVector or HLSUseSeqNumForIV must be configured. When HSS encryption is enabled, the HSSInitializationVector must be configured.</p>
HLSKeyRotationFragmentInterval	<p>Specifies the number of fragments after which a new encryption-key is used. We recommend rotating the keys every few minutes of fragments. The average size of a fragment can be used to configure this value; for example, if the average size of fragments is 6 seconds, and keys are rotated approximately every 5 minutes, then HLSKeyRotationFragmentInterval should be configured as 50.</p> <p>The range is from 0 to 5000. The default is 0 (zero). Following is an example of this parameter:</p> <pre>&lt;SetParameter name="HLSKeyRotationFragmentInterval" value="50" /&gt;</pre>

**Table F-2** SetParameter Name and Values for Session tracking and Session-Based Encryption (continued)

Name	Value
HLSMaxKeysPerSession	<p>When key rotation is enabled, this parameter specifies the total number of unique keys that are used for a playout session. The keys are re-used after the number of times that is derived by multiplying the HLSMaxKeysPerSession value by the HLSKeyRotationFragmentInterval value. A lower value ensures fewer keys are maintained per session on the Key Server. A higher value increases the probability that keys are not re-used within a session.</p> <p>The range is from 1 to 100. The default is 1.</p> <p>The average values of playout session duration and key rotation interval are taken into account to configure this value. For example, if we intend to rotate keys every 5 minutes, we need 12 keys per hour. So, a default value of 24 indicates, keys are re-used approximately after 2 hours of play-time.</p> <p>Following is an example of this parameter:</p> <pre>&lt;SetParameter name="HLSMaxKeysPerSession" value="10" /&gt;</pre> <p><b>Note</b> The HLSMaxKeysPerSession is mandatory if HLS encryption is enabled.</p>
KeyProfileIdleTimeout	<p>Used to clear the key profile that has no active connections. The range is from 600 to 86400 seconds. The default is 21600. Following is an example of this parameter:</p> <pre>&lt;SetParameter name="KeyProfileIdleTimeout" value="700" /&gt;</pre>
HLSInitializationVector	<p>A 16-byte ASCII string that is used for AES-128 encryption. Following is an example of this parameter:</p> <pre>&lt;SetParameter name="HLSInitializationVector" value="00000000000000000000000000000000" /&gt;</pre> <p><b>Note</b> If HLS encryption is enabled, the HLSInitializationVector or HLSUseSeqNumForIV must be configured.</p>
HLSUseSeqNumForIV	<p>Enables or disables using the HLS sequence number when the initialization vector attribute is not included in the EXT-X-KEY tag. A value of 1 means enabled. A value of 0 (zero) means disabled. The default is enabled. Following is an example of this parameter:</p> <pre>&lt;SetParameter name="HLSUseSeqNumForIV" value="1" /&gt;</pre> <p><b>Note</b> If HLS encryption is enabled, the HLSUseSeqNumForIV or HLSInitializationVector must be configured.</p>
HSSInitializationVector	<p>A 16-byte ASCII of the initialization vector used for AES-128 encryption. Following is an example of this parameter:</p> <pre>&lt;SetParameter name="HSSInitializationVector" value="00000000000000000000000000000000" /&gt;</pre> <p><b>Note</b> HSSInitializationVector is mandatory when HSS encryption is enabled.</p>
SessionResolveRule#integer	<p>At least one SessionResolveRule needs to be configured. A maximum of ten rules are supported, from SessionResolveRule#1 to SessionResolveRule#10. Following is an example of this parameter:</p> <pre>&lt;SetParameter name="SessionResolveRule#1" value="m3u8:none" /&gt;</pre> <p>For more information, see the “Session Resolve Rule” section on page F-16.</p>

**Table F-2 SetParameter Name and Values for Session tracking and Session-Based Encryption (continued)**

Name	Value
HLSKeyAcquisitionProfile HSSKeyAcquisitionProfile	Points to the Key Server profile that needs to be used for the ABR session to get the encryption key. Following are examples of these parameters:  <SetParameter name="HLSKeyAcquisitionProfile" value="AlphaKMS" /> <SetParameter name="HSSKeyAcquisitionProfile" value="CV-KMS" />
KeyProfile#integer	A maximum of ten KeyProfiles can be configured from KeyProfile#1 to KeyProfile#10. Following is an example of this parameter:  <SetParameter name="KeyProfile#1" value="ProfileName">  The value of the KeyProfile must match the value of either the HLSKeyAcquisitionProfile or the HSSKeyAcquisitionProfile.  The KeyProfile may exist without encryption enabled, but it will not be used.  For more information, see the <a href="#">“Key Management Server Interface” section on page F-18</a> .
KeyProfileValue#Create	Key Creation format template that is filled before sending the request to the KMS. This is an optional template. When not configured, it is expected that the KMS has already generated the keys for the user sessions.  The <i>KeyProfileValue</i> is the value of the KeyProfile. Following is an example of the KeyProfile# with the value “ProfileName,” and the #Create that specifies the “ProfileName” as the <i>KeyProfileValue</i> :  <SetParameter name="KeyProfile#1" value="ProfileName"> <SetParameter name="ProfileName#Create" value="POST, https://sjc-lds-214.cisco.com:4043/cgi-bin/keygen?r=<CONTENT-ID>&t=VOD&p=<CO UNT>" />  For more information, see the <a href="#">“Key Management Server Interface” section on page F-18</a> .
KeyProfileValue#Request	Key Request format template that is filled before sending the request to the KMS.  The <i>KeyProfileValue</i> is the value of the KeyProfile. Following is an example of the KeyProfile# and the #Request parameters:  <SetParameter name="KeyProfile#1" value="ProfileName"> <SetParameter name="ProfileName#Request" value="GET, https://sjc-lds-214.cisco.com:4043/cgi-bin/keygen?r=<CONTENT-ID>&p=<REKEY-IN DEX>&t=VOD" />  <b>Note</b> The Key Request template is mandatory if the KeyProfile#integer is configured.  For more information, see the <a href="#">“Key Management Server Interface” section on page F-18</a> .
KeyProfileValue#Delete	Key Delete format template that is filled before sending a delete message to the KMS. This is an optional template. Following is an example of the KeyProfile# and the #Delete parameters:  <SetParameter name="KeyProfile#1" value="ProfileName"> <SetParameter name="ProfileName#Delete" value="DELETE, https://sjc-lds-214.cisco.com:4043/cgi-bin/keygen?r=<CONTENT-ID>&t=VOD" />  For more information, see the <a href="#">“Key Management Server Interface” section on page F-18</a> .

**Table F-2 SetParameter Name and Values for Session tracking and Session-Based Encryption (continued)**

Name	Value
KeyProfileValue#LocalKeyURI	<p>Local Key URI format template is used to construct the key URI, which is used by clients to request the key from the KMS. If configured, it must respect the URI format generated by the KMS. If not configured, the SE will retrieve it from the KMS. Following is an example of the KeyProfile# and the #LocalKeyURI parameters:</p> <pre>&lt;SetParameter name="KeyProfile#1" value="ProfileName"&gt; &lt;SetParameter name=" ProfileName#LocalKeyURI" value="https://sjc-lds-214.cisco.com:4043/cgi-bin/keygen?r=&lt;CONTENT-ID&gt; &amp;t=VOD&amp;p=&lt;REKEY-INDEX&gt;" /&gt;</pre> <p>For more information, see the “<a href="#">Key Management Server Interface</a>” section on <a href="#">page F-18</a>.</p>
SessionNotificationFormat#integer	<p>A maximum of five session notifications formats can be configured, from SessionNotificationFormat#1 to SessionNotificationFormat#5.</p> <p>The value of the SessionNotificationFormat parameter is the following:</p> <pre>&lt;Format Name&gt;, Method, &lt;Body Format&gt;</pre> <p>The Format Name must be a non-empty string, the Method is either POST or GET, and the Body Format is an optional string.</p> <p>Following is an example of this parameter:</p> <pre>&lt;SetParameter name="SessionNotificationFormat#1" value="vc-start-stop-msg-1, POST, &lt;SessionNotif&gt; &lt;br&gt; &lt;SessionID&gt; %SESSION-ID% &lt;/SessionID&gt; &lt;br&gt; &lt;ClientIP&gt; %CLIENT-IP% &lt;/ClientIP&gt; &lt;br&gt; &lt;/SessionNotif&gt; &lt;br&gt;" /&gt;  &lt;SetParameter name="SessionNotificationFormat#2" value="vc-start-stop-msg-1, POST" /&gt;</pre> <p>For more information, see the “<a href="#">Session Start and Stop Notification Configuration</a>” section on <a href="#">page F-17</a>.</p>
SessionStartNotification#integer	<p>A maximum of five start notifications can be configured, from SessionStartNotification#1 to SessionStartNotification#5.</p> <p>The value of the SessionStartNotification parameter is the following:</p> <pre>&lt;Format Name&gt;, &lt;URL&gt;</pre> <p>The Format Name must be a non-empty string, and the URL must be a valid URL string. Both HTTP and HTTPS are supported, and the domain name or the IP address of the server can be specified. An empty message body can be sent. The information can be sent in a URL query string.</p> <p>Following is an example of this parameter:</p> <pre>&lt;SetParameter name="SessionStartNotification#1" value="vc-start-stop-msg-1, http://naveenpk.cisco.com:6666/cgi-bin/ssm" /&gt;</pre> <p>For more information, see the “<a href="#">Session Start and Stop Notification Configuration</a>” section on <a href="#">page F-17</a>.</p>

**Table F-2 SetParameter Name and Values for Session tracking and Session-Based Encryption (continued)**

Name	Value
SessionStopNotification#integer	<p>A maximum of five stop notifications can be configured, from SessionStopNotification#1 to SessionStopNotification#5.</p> <p>The value of the SessionStartNotification parameter is the following:</p> <pre>&lt;Format Name&gt;, &lt;URL&gt;</pre> <p>The Format Name must be a non-empty string, and the URL must be a valid URL string. Both HTTP and HTTPS are supported, and the domain name or the IP address of the server can be specified. An empty message body can be sent. The information can be sent in a URL query string.</p> <p>Following is an example of this parameter:</p> <pre>&lt;SetParameter name="SessionStartNotification#1" value="vc-start-stop-msg-1, http://naveenpk.cisco.com:6666/cgi-bin/ssm "/&gt;</pre> <p>For more information, see the “<a href="#">Session Start and Stop Notification Configuration</a>” section on page F-17.</p>
GenericSessionPlay#integer (RegEx)	<p>The regular expressions used to identify a session play. This is not a mandatory rule, if not configured, no Session Play event will be triggered. A maximum of 10 rules can be configured, named from “GenericSessionPlay#1” to “GenericSessionPlay#10”.</p> <p>Following is an example of this parameter:</p> <pre>&lt;SetParameter name="GenericSessionPlay#1" value="/play" /&gt;</pre>
SessionBitrate#integer (RegEx)	<p>The regular expressions used to identify the session’s bitrate. This is not a mandatory rule, if not configured, no Session Bitrate shift events will be triggered. A maximum of 10 rules can be configured, named from “SessionBitrate#1” to “SessionBitrate#10”. Following is an example of this parameter:</p> <pre>&lt;SetParameter name="SessionBitrate#1" value="/vod/(.*)/:bitrate=\$1"/&gt;</pre> <p><b>Note</b> This rule cannot be combined and used in existing HSS tracking feature, HSS tracking has its own method to retrieve its bit rate information</p>
SessionProfile#integer (RegEx)	<p>The regular expressions used to identify the session’s profile which is the alphanumeric identifier for bitrate information. This is not a mandatory rule, if configured, no Session Bitrate shift events will be triggered when profile changes. A maximum of 10 rules can be configured, named from “SessionProfile#1” to “SessionProfile#10”. Following is an example of this parameter:</p> <pre>&lt;SetParameter name="SessionProfile#1" value="/vod/(.*)/:profile=\$1"/&gt;</pre>
SessionCustomParameter#integer (RegEx)	<p>The regular expressions used to match the CDN URL for custom parameters retrieval. A maximum of 10 rules can be configured, named from "SessionCustomParameter#1" to "SessionCustomParameter#10". Following is an example of this parameter:</p> <pre>&lt;SetParameter name="SessionCustomParameter#1" value=".dp=(.*)&gt;~(.*)dp=\$1" /&gt;</pre>

**Table F-2 SetParameter Name and Values for Session tracking and Session-Based Encryption (continued)**

Name	Value
GenericSessionAccessProtect#integer(RegEx)	<p>The regular expressions used to identify the content access protect scope. A maximum of 10 rules can be configured, named from "GenericSessionAccessProtect#1" to "GenericSessionAccessProtect#10".</p> <p>Following is an example of this parameter:</p> <pre>&lt;SetParameter name=" GenericSessionAccessProtect#1 " value="/sample/.*.ts:none" /&gt;</pre> <p><b>Note</b> Starting from release 3.3, VDS-IS is enhanced to provide ability to reject requests with 403 response when fail to track the request in session and the requested content is protected.</p>
SCURLRegex#integer (RegEx)	<p>The regular expressions that will be used to identify Snapshot Counter URL group. At least 1 rule is mandatory.</p> <p>A maximum of 10 rules can be configured, named from "SCURLRegex#1" to "SCURLRegex#10".</p> <pre>&lt;SetParameter name=" SCURLRegex#1" value="m3u8" /&gt;</pre>
SCURLReportInterval#integer	<p>This knob is to configure the report interval for the corresponding SCURLRegex. A maximum of 10 rules can be configured, named from "SCURLReportInterval#1" to "SCURLReportInterval#10".</p> <p>Value: [1-10]</p> <p>Default value = 5</p> <pre>&lt;SetParameter name=" SCURLReportInterval#1" value="5" /&gt;</pre> <p> <b>Note</b> If there is no corresponding knob SCURLReportInterval for knob SCURLRegex, the default report interval is 5 mins.</p>
SCURLIgnoreQS#integer (Flag)	<p>This knob to control the corresponding SCURLRegex whether to exclude query string parameters as part of the regexp match.</p> <p>A maximum of 10 rules can be configured, named from "SCURLIgnoreQS#1" to "SCURLIgnoreQS#10".</p> <p>Value: On, Off</p> <p>Default value = Off</p> <pre>&lt;SetParameter name=" SCURLIgnoreQS#1" value="1" /&gt;</pre> <p> <b>Note</b> If there is no corresponding knob SCURLIgnoreQS for knob SCURLRegex, the default behavior is to exclude the query string parameters for the SCURLRegex.</p>

## Session Resolve Rule

The SessionResolveRule is used to extract session information, such as session ID and client IP address, from the request URL. The request URL is sent by the client to retrieve the manifest and content fragments. Each request URL has a query string that specifies the session ID, client IP address, and other session information, which can be used to look up and validate the session.

The SessionResolveRule is a pattern-matching rule that uses a regular expression to resolve an HTTP request to the associated session. The SessionResolveRule can be used for the following situations:

- Detect the start of a playout session, if the start information does not exist
- Track a session by identifying the parameters that define a unique session

To support different ABR protocols with different patterns in the same Delivery Service, separate session-resolve rules can be configured.

The SessionResolveRule is specified as a string with the following substrings:

```
<regex-match-string>:<output-string>
```

The regex-match-string is the pattern that the URL must match. Either the manifest URL must match the pattern, or both the manifest and fragment URL must match.

The output-string is the list of attributes to extract. Each attribute is separated by a tilde (~), also known as the approximate symbol. The format and attribute names are the same as the session cookie. The output-string can contain the following attributes:

- sid—Session identifier
- cip—Client IP address



**Note** The attribute retrieved from URL in output string is used as session attribute. We highly recommend that you do not add a duplicate attribute as it causes confusion.

To specify no output-string, use the word *none*. An example follows:

```
<SetParameter name="SessionResolveRule#1" value="m3u8:none" />
```

Following are some examples of the SessionResolveRule:

- Detect the start of a session and extract the session ID.

```
SessionResolveRule#1: "SID=(.*)&.*CIP=(.*)&:sid=$1~cip=$2"
URL:
/NBCHD/index.m3u8?SID=4e4c2bf5734fdf0f88b9aa56bc240882&IS=0&ET=1237958266&CIP=64.102.2
42.2&KO=1&KN=1&US=9994d7f80b4c68b2e6b9e5c590ab6ad7
Output-string: sid=4e4c2bf5734fdf0f88b9aa56bc240882~cip=64.102.242.2
```

- If external system generates a customized manifest file or each client, the session tracking information is contained in the query string for the manifest and fragment requests. The SessionResolveRule is specified as follows:

```
SessionResolveRule#1: "sessionid=(.*)&ipaddress=(.*)&:sid=$1~cip=$2"
URL:
/uploads/cbshd/20110323T162152-01-1105378.ts?cdnHost=167.206.237.22&sessionid=39865970
1312384582563&ipaddress=64.102.242.2&callsign=CBSHD&zipcode=11797&hubid=4&fta=23&optim
umid=webdvr1ad&devicename=&devicetype=0&osver=null&res=HD
Output-string: sid=398659701312384582563~cip=64.102.242.2
```

- If the session ID is not assigned by an entitlement server, a unique session ID is generated by the VDS-IS. In this case, the SessionResolveRule is only used to detect the start of a session. Requests are tracked by enabling cookie tracking.

```
"SessionResolveRule#1: "m3u8:none"
URL: /NBCHD/index.m3u8
Output-string: none
```

## Session Start and Stop Notification Configuration

This section describes the format definitions for the start and stop notifications, the configuration of these notifications, and monitoring session notification messages.

### Start and Stop Notification Format Definition

The SessionNotificationFormat parameter defines the format for the start and stop notifications. A maximum of five notification formats can be defined for different KMSs. The format definition is composed of the following elements:

- Format name—Name of the format is a required string
- HTTP method—Either POST or GET
- Format body—Contains one or more tokens that can map to the parameters of a session. The tokens are replaced with actual values for the session occurring at the time the notification is sent. The format body is optional. If the format body is not included, the tokens are specified in the URL query string.

The format body tokens can be one or more of the following:

- %SESSION-ID%—External or internal session ID
- %FLOW-ID%—Five-tuple consisting of SourceIP-SourcePort-DestIP-DestPort-Protocol
- %CLIENT-IP%—Client IP address associated with the session
- %LAST-REQ-URL%—Last requested URL

Following are two examples of the SessionNotificationFormat parameter:

```
<SetParameter name="SessionNotificationFormat#1" value="vc-start-stop-msg-1, POST,
<br>&lt;SessionNotif&gt; &lt;br&gt; &lt;SessionId&gt; %SESSION-ID% &lt;/SessionID&gt;
&lt;br&gt; &lt;ClientIP&gt; %CLIENT-IP% &lt;/ClientIP&gt; &lt;br&gt; &lt;/SessionNotif&gt;
&lt;br&gt;" />

<SetParameter name="SessionNotificationFormat#2" value="vc-start-stop-msg-2, POST" />
```

### Per-Delivery Service Start and Stop Notification Configuration

The SessionStartNotification and the SessionStopNotification reference the format defined in the SessionNotificationFormat parameter. So, the *Format-Name* must match a *Format-Name* in the SessionNotificationFormat definition. The format definition is retrieved for the start or stop notification, and the configured Method is performed for the URL specified in the notification.

Following is the syntax or the start and stop notifications:

```
SessionStartNotification#x = "<Format-Name>, <URL>"
SessionStopNotification#x = "<Format-Name>, <URL>"
```

Following are examples of the start and stop notifications using the vc-start-stop-msg-1 format:

```
<SetParameter name="SessionStartNotification#1" value="vc-start-stop-msg-1,
http://naveenpk.cisco.com:6666/cgi-bin/ssm"/>
```

## Configuring Session-Based Encryption and Session Tracking

```
<SetParameter name="SessionStopNotification#1" value="vc-start-stop-msg-1,
http://naveenpk.cisco.com:6666/cgi-bin/ssm"/>
```

Following are examples of the start and stop notifications using the vc-start-stop-msg-2 format, which does not specify the format body, but instead specifies the URL query string in the URL:

```
<SetParameter name="SessionStartNotification#2" value="vc-start-stop-msg-2,
http://naveenpk.cisco.com:6666/cgi-bin/ssm?sessionid=%SESSION-ID%&ipaddress=%CLIENT-IP%
%"/>
```

```
<SetParameter name="SessionStopNotification#2" value="vc-start-stop-msg-2,
http://naveenpk.cisco.com:6666/cgi-bin/ssm?sessionid=%SESSION-ID%&ipaddress=%CLIENT-IP%
%&url=%LAST-REQ-URL%"/>
```

### Monitoring Session Notification Messages

Start and stop notification messages track the session creation and deletion on the SE and convey the same to the configured session state manager server.

The start notification message is sent after the session has been successfully created. The stop notification message is sent when the session is deleted, which occurs when the session has been inactive for the length of time that is defined in the SessionIdleTimeout parameter specified in the Service Rule file. Session start and stop notifications are best-effort services. If the SE fails to send the message, or an error response is received from the session state manager server, it is ignored and client continues to be served.

Following counters have been added to track the notification messages:

- Start Notifications sent—Number of start notification messages sent out successfully from the SE
- Start Notification send failed—Number of start notification messages that were not sent out because of an internal failure on the SE
- Stop Notifications sent—Number of stop notification messages sent out successfully from SE
- Stop Notification send failed—Number of stop notification messages that were not sent out because of an internal failure on the SE

The counters for HLS sessions are displayed in the output of the **show statistics web-engine abr hls-media-app session** command.

The counters for HSS sessions are displayed in the **show statistics web-engine abr smoothhd-media-app session** command.

The counters for Generic sessions are displayed in the **show statistics web-engine abr generic-session-app session** command.

## Key Management Server Interface

The Key Management Client (KMC) module on the SE uses HTTP or HTTPS to retrieve the session-based encryption keys from the KMS. For HLS, the KMC uses the published interface of the KMS to retrieve the 128-bit AES key and the key URI that is sent to the client.

To display the key statistics for the SE, use the **show statistics web-engine key-client** command.

### Key Profile Template Configurations in Service Rule File

Because the VDS-IS integrates with different KMSs, each with a different interface, the key profile templates provide a way to configure messages for each KMS.

The following rules apply to key profiles:

- Each key profile is associated with a specific KMS and the messages accepted by that key server (Create is a POST, Request is a GET, and Delete is a DELETE).
- Each Delivery Service can have up to ten key profiles.
- Each SE supports up to 100 key profiles.
- Key profiles are not associated with an application or protocol

The following parameters for the SetParameter element in the Service Rule file are used to configure the messages to each KMS:

- KeyProfile#—Defines a name for the KMS profile
- #Create—Defines a create key message (POST) for the KMS profile specified
- #Request—Defines a request key message (GET) for the KMS profile specified
- #Delete—Defines a delete key message (DELETE) for the KMS profile specified
- #LocalKeyURI—Used to generate the key URI locally in the SE and sent in the manifest to the client; instead of getting the key URI from the KMS

The #Create, #Request, #Delete, and #LocalKeyURI must have the KeyProfile# name prefix, and the value must have the HTTP method followed by a comma and the URL.

Following are examples of the key messages for the AlphaKMS key profile:

```
<SetParameter name="KeyProfile#1" value="AlphaKMSS" />
<SetParameter name="AlphaKMS#Create" value="POST,
https://sjc-lds-214.cisco.com:4043/cgi-bin/keygen?r=<CONTENT-ID>&t=VOD&p=<COUNT>" />
<SetParameter name="AlphaKMS#Request" value="GET,
https://sjc-lds-214.cisco.com:4043/cgi-bin/keygen?r=<CONTENT-ID>&p=<REKEY-INDEX>&t=VOD" />
<SetParameter name="AlphaKMS#Delete" value="DELETE,
https://sjc-lds-214.cisco.com:4043/cgi-bin/keygen?r=<CONTENT-ID>&t=VOD" />
<SetParameter name="AlphaKMS#LocalKeyURI"
value="https://sjc-lds-214.cisco.com:4043/cgi-bin/keygen?r=<CONTENT-ID>&t=VOD&p=<REKEY-IND
EX>" />
```

The URLs specified in the #Create, #Request, #Delete, and #LocalKeyURI have the following tokens that are replaced with the values of the current session:

- <SESSION-ID>—Session ID of the session. For the external session ID, the external session ID is sent as received in the original request without any Delivery Service prefix. For the internal session ID, the full ID with the Delivery Service prefix is sent.
- <CONTENT-ID>—Hash (32 bytes) of the session ID.
- <CLIENT-IP>—Client IP address that could be used for any validation by the KMS.
- <REKEY-INDEX>—Index value of the key for a given session, used for key rotation.
- <COUNT>—Maximum number of keys, used for key rotation.

### Key Creation Message from SE

The key creation message is used when the KMS requires keys to be pre-created and reserved for a channel or media. The key creation message has any of the five tokens required by the KMS, but typically includes the following fields:

## Configuring Session-Based Encryption and Session Tracking

Field Name	Value Range	Description
CONTENT-ID	0–4294967295	Identifier of a specific content for which the key is needed. For media-based-encryption, this maps to MediaID (ChannelID or VOD). For session-based-encryption, this maps to user-session-identifier.
COUNT	0–100	Maximum number of keys to generate. If there is a configurable limit on the KMS, then this value is bounded by that value.

For HLS, the key count is configured in the HLSMaxKeysPerSession parameter. For HSS, the key count is always 1. If the KMS relies on another mechanism to create the session key, the key creation message is not sent from the SE.

An example of the value field of the key creation message SetParameter follows:

```
POST, https://naveenpk.cisco.com:4430/cgi-bin/keygen?r=<SESSION-ID>,&t=VOD&p=<COUNT>;"
```

An example of successful key creation response follows:

```
HTTP/1.1 200 OK
Date: Mon, 30 Apr 2012 16:41:30 GMT
Server: Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.7a
Accept-ranges: none
Last-Modified: Mon, 30 Apr 2012 16:41:30 GMT
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-1
Length: 0 [text/html]
```

### Key Request Message from SE

The key request message includes the following fields:

Field Name	Value Range	Description
CONTENT-ID	0–4294967295	Identifier of a specific content for which the key is needed. For media-based-encryption, this maps to MediaID (ChannelID or VOD). For session-based-encryption, this maps to user-session-identifier.
REKEY-INDEX	0–100	Rekey index maps to a different key within the key set. If COUNT=N is specified at key creation time, this value is in the 0 to N-1 range.

An example of the value field of the key request message SetParameter follows:

```
GET, https://naveenpk.cisco.com:4430/cgi-bin/keygen?r=<SESSION-ID>,&t=VOD&p=<REKEY-INDEX>;"
```

An example of successful key request response follows:

```
HTTP/1.1 200 OK
Date: Mon, 30 Apr 2012 16:33:58 GMT
Server: Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.7a
Pragma: no-cache
```

```

Accept-ranges: none
Content-length: 16
Last-Modified: Mon, 30 Apr 2012 16:33:58 GMT
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: binary/octet-stream
Length: 16 [binary/octet-stream]

```

0123456789abcdef0123456789abcdef

Response code “201 OK” and “201 Created” also signify success.

The key-request response message includes the following fields:

Field Name	Value Range	Description
KEY-LENGTH	NN	For HLS, this field always has the numeric value 16.
PLAYER-URL	STRING	Key retrieval URL presented to the client by way of the application playlist. The PLAYER-URL is the location field in the HTTP header.
KEY	ANY	A 16-byte octet string used to encrypt or decrypt content. The KEY is in the body of the HTTP reply.

### Key Deletion Message from SE

The key deletion message is required by the KMS, when keys are pre-created with a create message. The key deletion message consists of any of the five tokens.

An example of the value field of the key deletion message SetParameter follows:

DELETE, [https://naveenpk.cisco.com:4430/cgi-bin/keygen?r=<SESSION-ID>&t=VOD"](https://naveenpk.cisco.com:4430/cgi-bin/keygen?r=<SESSION-ID>&t=VOD)

An example of successful key deletion response follows:

```

HTTP/1.1 200 OK
Date: Mon, 30 Apr 2012 16:56:59 GMT
Server: Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.7a
Accept-ranges: none
Last-Modified: Mon, 30 Apr 2012 16:56:59 GMT
Content-Length: 0
Content-Type: text/html; charset=ISO-8859-1
Length: 0 [text/html]

```

## Transaction Logs for Session-Based Encryption and Session Tracking

Transaction logs for Session-Based Encryption and Session Tracking consist of the following:

- [Key Client Manager Transaction Logs](#)
- ABR and Generic Session transaction logs

For more information on ABR and Generic Session transaction logs, see the “[Web Engine User Level Session Transaction Logs](#)” section on page 8-96..

**Key Client Manager Transaction Logs**

The Key Client Manager (KCM) transaction logs capture the details of the transactions between the KMS and the SE. When transaction logging is enabled, transaction logs between the SE and KMS are logged in the KeyClientManager log file in the /local/local1/logs/KeyClientManager/ directory.

Table F-3 describes the KCM transaction log fields.

**Table F-3 KCM Transaction Log Fields**

Field	Description
Timestamp	Time stamp of the transaction.
Session_ID	ID of the session.
Key_Server	Domain or IP address of the KMS.
Key-Profile#DsId	Key profile name used in this transaction.
HTTP-Method	HTTP method used in the transaction (POST, GET, or DELETE).
Key-Request-URL	URL of HTTP call sent to the KMS in this transaction.
Response-Status	Status of transaction.
Key-URI	Client key URI that is inserted in manifest file. The end-user client uses this URL to acquire the key from the KMS.



## Creating NAS Files

---

This appendix describes the Network Attached Storage (NAS) feature. This appendix consists of the following topics:

- [Introduction, page G-1](#)
- [Creating a NAS XML File, page G-4](#)
- [NAS XML File Example, page G-4](#)

## Introduction

Network-attached Storage (NAS) is supported as a read-only storage repository at the root location (Content Acquirer) in the Videoscape Distribution Suite, Internet Streamer (VDS-IS). Content is written to the NAS by an external agent, such as the Origin Server, a publishing subsystem, or a data storage application. The NAS offers a “new content category,” similar in characteristics to dynamically-cached content, which does not require metadata attachment.



---

**Note** NAS is only supported in lab integrations as proof of concept.

---

The following rules apply to NAS support:

- NAS cannot be used as a source for prefetched or hybrid content.
- Only content serviced by the Web Engine is supported (HTTP content and Flash Media Streaming).



---

**Note** NAS for Windows Media Streaming and Movie Streamer is not supported.

---

- Only Network File System (NFS) mounts are supported for acquiring content from the NAS.
- Content acquired from the NAS is not written to local storage on the SEs at the root location; when reading content, NAS is considered an extension of the local file system.
- If there is more than one SE in a root location for a Delivery Service, then the SE that acquires the content from NAS is based on a hash of the content URL (similar to dynamically-cached content).
- NFS share can be mounted from multiple IP addresses simultaneously.
- Multiple mounts for the same volume on a NAS is supported.
- NAS should be colocated with the SEs at the root location; if WAN link is used, then WAN link failover scenario should be provided.

- IP address failover by the NAS should be implemented to avoid service disruption.
- NAS is not applicable to live streaming
- NAS lookup is tried before pulling content from the Origin Server
- When Web Engine performs FastCAL lookup, NAS file lookup is performed first; followed by cached content, then prefetched content.
- In a cache-miss scenario, the Origin Server is queried last.

**Note**

Ingress traffic from NAS mounts is not distributed evenly over port channels. Separate interfaces can be used for NAS outside of the port-channel configuration to achieve better load balancing. Ingress traffic to the VDS-IS is determined by the switch, this applies to all application traffic over port channels.

Network traffic performance can be impacted by too small a value for the TCP parameter: net.inet.tcp.rexmit\_slop. If it is determined that network throughput performance is impacted, the net.inet.tcp.rexmit\_slop value on the NAS server should be reviewed.

The permissions for directories on the NAS-mounted file system should be a minimum of “read” and “execute” by *others*, and files on the NAS-mounted file system should be a minimum of “read” by *others*.

For example, a directory permission at a minimum should be:

`dr-xr-xr-x`

and a file permission at a minimum should be:

`-r--r--r--`

If access to a NAS-mounted content results in a 500 error, the permissions of the files should be verified.

## Reading NAS Metadata

Metadata for content stored on network-attached storage (NAS) devices is now fetched. Metadata is associated with a content file. The metadata for a content file is stored as <file>.metadata, in the same directory as the content file. For example, if the content file is located at /datap1/vod/flv/sample.flv, the metadata file is located at /datap1/vod/flv/sample.flv.metadata.

**Note**

NAS is only supported in lab integrations as proof of concept.

It is assumed that the content store (NAS) has the metadata of the content that is to be stored as a separate file with name such as <content\_name>.metadata in the same directory location. It is also assumed that the format of the file complies with the following rules:

- File format is a simple text file with each line of the file having an attribute name and an associated attribute value separated by a colon (:). No spaces are allowed anywhere in the metadata file. Format and pattern for the metadata file is as follows:
  - <attribute1>:<value1>
  - <attribute2>:<value2>
  - <attribute3>:<value3>
- Basic attributes supported are as follows:
  - expires

- s-maxage
- max-age
- must-revalidate
- proxy-revalidate
- etag
- content-type
- content-encoding
- age
- retry-after

Any header attributes other than the basic attributes listed are considered custom and are written into the client response header.

## Configuring NAS

Configuring NAS in the VDS-IS consists of the following tasks:

1. Create a NAS XML file.
2. Register a NAS XML file with the CDSM by uploading or importing the file.
3. Associate a NAS XML file with a content origin.

For information on registering a NAS file, see the “[NAS File Registration](#)” section on page 6-16. For information on associating a NAS XML file with a content origin, see the “[Content Origins](#)” section on page 5-1.

## NAS Mount Removal

When removing NAS mounts, the SE configuration should be updated before the NAS IP addresses are removed.



**Note** Any NAS mount changes should be performed in a maintenance window to avoid service disruption.

To remove NAS mounts, follow these steps:

- 
- Step 1** Remove from the NAS XML file the IP addresses that are to be removed from the NAS server.
- Step 2** Update the NAS XML configuration file in the CDSM GUI.
- a. Register the updated NAS XML file with the CDSM by choosing **System > Configuration > NAS File Registration**.
  - b. Associate the NAS file with the Content Origin of the Delivery Service by choosing **Services > Service Definition > Content Origins**.
- Step 3** Verify the configuration has been propagated to each SE in the Delivery Service by entering the **show content-origin** command on each SE in the Delivery Service.
- Step 4** Remove the IP addresses on the NAS server.
-

# Creating a NAS XML File

The XML Schema file describes and dictates the content of the XML file. The CdsOrigin.xsd file contains the XML schema. To view or download a copy of the CdsOrigin.xsd file, see the “[Viewing or Downloading XML Schema Files](#)” section on page 6-24.

The NAS file can be created using any ASCII text-editing tool. Table 1 describes the NAS XML file elements. The NAS

**Table 1** *NAS XML File Elements*

Element	Subelements	Attributes	Description
CdsOrigin	server	name	Name for the NAS server. This is used as an internal reference.
		host	Domain name or IP address of NAS server.
	sourceNFS	name	Internal name reference used on the localMount section as the “source.”
		sharePoint	Exported file system from the NAS server.
		access	Mount option, only “ro” read-only is supported.
		maxRetry	Number of retries performed on a failed mount point before raising the alarm from a minor to major severity.
		rsize	Maximum negotiated buffer size between the SE and the NAS server.
	localMount	name	Name of the local mount. This is used as an internal reference.
		source	Reference to the sourceNFS subelement name.
		mountPoint	Defines the local mount point base.
		num-of-mounts	Number of mount points to be used from the serverList. This number cannot be greater than the number of entries in serverList.
		order	Defines how the servers in the serverList are selected: <ul style="list-style-type: none"> <li>• fcfs —Use the first num-of-mounts from the serverList</li> <li>• random—Randomly select the servers to use from the serverList</li> </ul>
		serverList	List of servers to use from the servers defined in the server subelement. List is comma delimited, or comma and space delimited.

## NAS XML File Example

Following is an example of the NAS XML file:

```
<?xml version="1.0"?>
<CdsOrigin>
    <server name="nas1" host="192.168.252.67"/>
    <server name="nas2" host="192.168.252.68"/>
    <sourceNFS name="NAS" sharePoint="nas_nfs" access="ro" maxRetry="10" rsize="131072"/>
    <localMount name="localMount" mountPoint="vod" source="NAS" num-of-mounts="2"
      order="fcfs" serverList="nas1, nas2"/>
</CdsOrigin>
```



# URL Signing and Validation

This appendix describes the URL signing and validation method for the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS). This appendix contains the following sections:

- [Introduction, page H-1](#)
- [Configuring the VDS-IS for URL Signing, page H-3](#)
- [URL Signing and Validating, page H-6](#)

## Introduction

The VDS-IS accepts and fulfills requests for video content from client devices in the form of content URLs. Content and service providers, to protect their copyright and fulfill their licensing obligations, often need to restrict access to content and limit viewing times. Basic authentication and authorization at the portal (for example, username and passwords) can help achieve this objective by restricting content access to authorized users. However, because URLs are inherently open, users (once authenticated at the portal) could potentially share these content URLs with other possibly unauthorized users, or continue to access the content beyond the allotted time.

The VDS-IS provides the infrastructure to sign and validate content URLs, restricting access to some users and limiting viewing times.

## URL Signing Components

One of the easiest ways to restrict content access to a particular user is to embed, within the content URL, the client IP address of the user for whom the content access was authorized. Similarly, to ensure that the content expires after a predetermined time, an expiry timestamp could be embedded. These values can then be validated against the actual client sending the request and the current time at the Service Engine serving the request. If either of the two validations fail, the request is rejected.



**Note** You can exclude the checks for the client IP address and the content expiry by configuring a Service Rule on each SE. For more information, see the “[Configuring Service Rules](#)” section on page 4-21.

However, because any of these strings in the URL could potentially be edited manually and circumvented by any knowledgeable user, it is important to generate and attach a signature to the URL. This can be achieved by attaching a keyed hash to the URL, using a secret key shared only between the signer (the portal) and the validating component (VDS-IS).

VDS-IS has incorporated an open and well-documented signing mechanism that uses standard hashing schemes. The URL signing mechanism offers the flexibility to either use the provided signing script, or you can develop a signing application in the platform or language of your choice, as long as it adheres to the specified format.

For signing and validation of the URL, the VDS-IS relies on a set of one or more secret keys shared between the portal and the devices within the VDS-IS.

**Note**

Sometimes media players append the port number to the URL. In this case, the SE removes the port number from the URL before validating the signature.

## Supported Protocols and Media

The URL signing and validation is supported across all VDS-IS protocol engines: Windows Media Streaming engine, Movie Streamer engine, Flash Media Streaming engine, and Web Engine.

**Note**

Content-based routing does not work with clients sending signed URL requests. The hashing algorithm for content-based routing considers the whole signed URI, so a signed URL request for the same content may be redirected to a different SE.

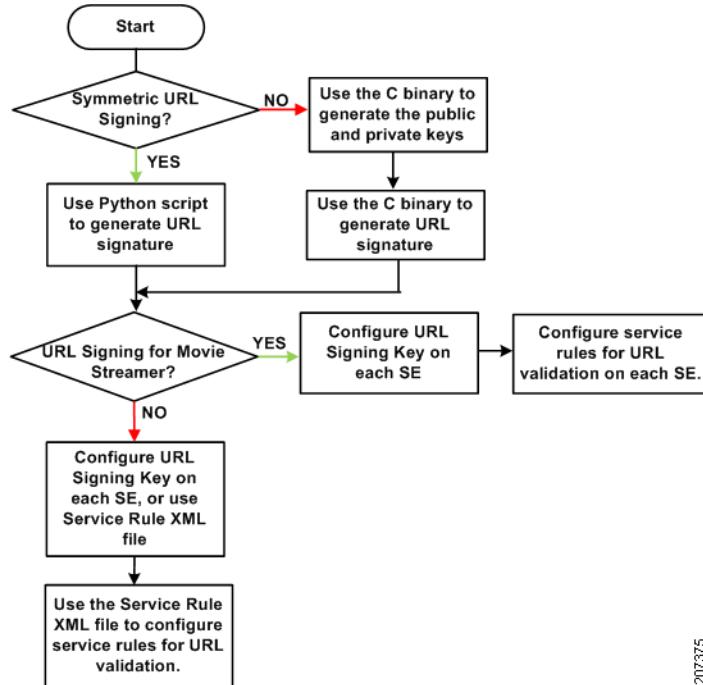
**Note**

URL validation for Web Engine HTTP requests, as well as Flash Media Streaming RTMP requests and Windows Media Streaming RTSP requests, is configured by using the Delivery Service Service Rule XML file. For more information, see [Appendix E, “Creating Service Rule Files.”](#)

# Configuring the VDS-IS for URL Signing

The URL signing and validation configuration requirements differ depending on the VDS-IS software release. [Figure H-1](#) describes the URL signing and validation workflow.

**Figure H-1 URL Signing and Validation Configuration Workflow**



207375

The VDS-IS URL signing infrastructure supports multiple keys. Different pieces of content, with different URLs, can be signed by different keys. Keys are stored as a key matrix and identified (indexed) by a key ID owner and a key ID number.

## Configuring URL Signing

Configuring the VDS-IS for URL signing and validation differs depending on the protocol engine.

### Configuring URL Signing for Movie Streamer

To enable validation of URLs for Movie Streamer, the following tasks must be completed on all participating Service Engines:

- Configure URL Signing
- Enable Service Rules processing
- Configure rules to validate URLs matching the below pattern-lists
- Configure pattern-lists to match URLs, domain names, or both

For information on configuring URL Signing, see the “[Configuring URL Signing Key](#)” section on [page 4-27](#). For information on enabling Service Rules processing and configuring Service Rules on each Service Engine, see the “[Configuring Service Rules](#)” section on [page 4-21](#).

### Configuring URL Signing for the Web Engine, Flash Media Streaming, and Windows Media Streaming

To enable validation of URLs for Web Engine, Flash Media Streaming, and Windows Media Streaming, the following tasks must be completed:

- Configure URL Signing on all participating Service Engines by using the **url-signature** command on each SE or the CDSM GUI URL Signing page for each SE. Alternatively, use the Service Rule XML file to configure URL Signing for each Delivery Service
- Enable Authorization Service on all participating Service Engines (enabled by default)
- Create a Service Rule XML file and upload it to each participating Delivery Service. The Service Rule XML file must have the following:
  - Rules to validate URLs matching the below pattern-lists
  - Pattern-lists to match URLs, domain names, or both
  - For Windows Media Streaming live .asx requests, you can include rules to generate URL signatures with pattern lists that must be matched

For information on configuring URL Signing for each Service Engine, see the “[Configuring URL Signing Key](#)” section on page 4-27. For information on creating the Service Rule XML file for validating the URL signatures and for configuring the URL signing for each Delivery Service, see the [Appendix E, “Creating Service Rule Files.”](#) For information on uploading the Service Rule XML file to the Delivery Service, see the “[Authorization Plugins](#)” section on page 5-27.

## Configuring Service Rules for URL Signing

Configure the Service Rules to validate the URL based on Service Routing Domain Name and the Origin Server FQDN, or the url-regex.

To configure the Service Rule for Movie Streamer, use one of the following methods:

- Using the CLI, each SE should contain at least one rule of the form:

```
rule action validate-url-signature pattern-list <n> protocol <protocol>
```

where pattern-list <n> will match the requests coming in from the clients.

Following is another example of using the CLI to configure the SE:

```
rule pattern-list 1 domain cds.cisco.com
rule action validate-url-signature error-redirect-url http://foobar.com pattern-list 1
protocol rtsp
rule enable
```

- In the CDSM GUI, choose **Devices > Service Control > Service Rules**, and click the **Create New** icon. From the **Rule Type** drop-down list, choose **pattern-list**. Enter parameters to match requests from the client. As an example, entering:

```
1 url-regex live
```

would cause pattern list 1 to match any request with the string “live” in the URL.

Click **Create New** again and this time from the **Rule Type** drop-down list, choose **validate-url-signature**. As an example, entering:

```
error-redirect-url <error_url> pattern-list <n> protocol rtmp
```

where the client is redirected to <error\_url> when the rule check fails, and pattern list <n> is the one you just created.

To configure Service Rules to validate the URL signature for Web Engine, Windows Media Streaming, or Flash Media Streaming, use the Service Rule XML file. An example of the Service Rule rule action for validating the URL signature follows:

```
<Rule_Validate matchGroup = "1" protocol = "http" error-redirect-url =
"http://wwwin.cisco.com" exclude-validation = "all" />
```

where the pattern list 1 will match HTTP requests coming in from the clients, if they do not match the client is redirected to the error URL, and the client IP address and the expiry time are excluded from the validation.

## Configuring URL Signing Key

Configure the URL signature with Key-Owner, Key-Number, and Key if you are using symmetric key signing. Make sure this database of keys is given to both the portal server and Origin server.

Whether you use the CDSM GUI, the CLI, or the Service Rule XML file, you must configure URL Signing in one of the following ways:

- In the CDSM GUI, for each SE choose **Devices > Service Control > URL Signing**, then click the **Create New** icon. From the **Cryptographic Algorithm** drop-down list, choose **Symmetric Key** or **Asymmetric Key**.
  - If you selected Symmetric Key, enter the Key ID Owner, Key ID Number, and Key. It is important that these values match those of the portal.
  - If you selected Asymmetric Key, enter the Key ID Owner, Key ID Number, the location of the Public Key file, and if used, the Private Key location and the Symmetric Key (AES encryption). For more information about the public key signing, see the “[Public Key URL Signing for Asymmetric Keys](#)” section on page [H-15](#).
- In the CLI, each SE must have a URL signing key enabled that matches the one in the portal's configuration file.

Adding keys:

```
url-signature key-id-owner 1 key-id-number 2 key "foobar"
```

Viewing keys:

```
# show url-signature
```

- For Web Engine, Flash Media Streaming, and Windows Media Streaming, you have the additional option of using the Service Rule XML file to configure the URL Signing on a per-Delivery Service basis.
  - Following is an example of symmetric key URL signing:

```
<CDSRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSRules.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Cisco</CustomerName>
  <ApplyAllTier>yes</ApplyAllTier>
  <Rule_Patterns>
    <PatternListGrp id = "grp1">
      <Domain>cds.cisco.com</Domain>
    </PatternListGrp>
  </Rule_Patterns>
  <Rule_Actions>
    <Rule_Validate matchGroup="grp1" key="cisco123" protocol="all"
error-redirect-url="http://wwwin.cisco.com" />
  </Rule_Actions>
</CDSRules>
```

```
</CDSRules>
```

For more information on configuring Service Rule XML files with URL Signing for both symmetric and asymmetric keys, see the “[URL Signing Key in the Service Rule File](#)” section on page E-18.

For information about asymmetric key signing, see the “[Public Key URL Signing for Asymmetric Keys](#)” section on page H-15.

## URL Signing and Validating

The VDS-IS software supports symmetric key URL signing and asymmetric key URL signing (also known as public key URL signing). Symmetric key signing uses the same key to sign and validate the URL. Asymmetric keys always have a key pair made up of a public key and private key. The private key is used for signing and the public key is used for validation.

Symmetric keys, which means the same key is used for both signature generation and validation, are known by both parties. There is the signature generator, usually the portal, and the signature validator, which is the VDS-IS. Symmetric keys use either the MD5 or the SHA1 hash algorithm. They must remain secret at both ends, because the same key is used for both signing and validation. The key should be changed frequently.

Asymmetric keys, which means a private key is used for signing and a public key is used for validation, need to secure only the private key end. Also, the public/private key pair can be used for a longer duration without having to change them.

This section contains the following topics:

- [URL Signing Script for Symmetric Keys](#)
- [Public Key URL Signing for Asymmetric Keys](#)

## URL Signing Script for Symmetric Keys

At the portal, URLs can be signed for a particular user (client IP address) and expiry time using a URL signing script. The URL signing script example included in this section requires Python 2.3.4 or higher.

You can also use the **url-signature** command to generate the URL signature for symmetric keys. For more information, see the “[url-signature Command](#)” section on page H-15. The CDSM GUI offers the ability to generate the URL signature for symmetric keys as well. See the “[Configuring URL Signing Key](#)” section on page 4-27 for more information about the **Key** field.

## URL Signing Version

The URL signing script offers three different versions:

- MD5 hash algorithm
- SHA-1 hash algorithm
- SHA-1 hash algorithm with the protocol removed from the beginning of the URL (without schema)

**Note**

A reason to use the SHA-1 hash algorithm with the protocol (schema) removed is when a URL is signed for RTSP and a player does a fallback to HTTP for the same URL. The validation fails because the URL signature includes RTSP. If the URL signature does not include the protocol, the fallback URL is validated correctly even though the protocol is HTTP.

**Version 0 or No Version Specified**

If you do not specify a version, or specify version 0, for the script, MD5 is used and the SIGV string in the script is not added.

Following is an example of the URL signing script using the MD5 security hash algorithm:

```
python cds-ims-urlsing.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 0
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?IS=0&ET=1241194518&CIP=8.1.0.4&KO=1&KN=2&US=deebacde45bf71  
6071c8b2fecaa755b9
```

**Version 1 Specified**

If you specify version 1 for the script, SHA-1 is used and the SIGV=1 string is added.

Following is an example of the URL signing script using the SHA-1 security hash algorithm:

```
python cds-ims-urlsing.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 0 1
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=1&IS=0&ET=1241194679&CIP=8.1.0.4&KO=1&KN=2&US=8349348  
ffac7987d11203122a98e7e64e410fa18
```

**Version 2 Specified**

If you specify version 2 for the script, SHA-1 is used. The protocol from the beginning of the URL is removed before the signature is generated, and the SIGV=2 string is added. The protocol is RTSP, HTTP, or RTMP. The URL is signed without the protocol, but the final signed URL is printed with the protocol.

Following is an example of the URL signing script using the SHA-1 security hash algorithm with version 2 specified:

```
python cds-ims-urlsing.py http://www.cisco.com/index.html 8.1.0.4 200000 1 2 cisco 0 2
```

An example of the resulting signed URL follows:

```
http://www.cisco.com/index.html?SIGV=2&IS=0&ET=1241194783&CIP=8.1.0.4&KO=1&KN=2&US=68b5f5e  
d97d1255a0ec42a42a4f779e794df679c
```

**Version 3**

Version 3 is used by the C binary in externally signing the URLs for the public/private key pairs. The protocol (schema) from the beginning of the URL is removed before the signature is generated, and the SIGV=3 string is added. For more information, see the “[Public Key URL Signing for Asymmetric Keys](#)” section on page [H-15](#).

## Example of a Python URL Signing Script

The following simple Python script demonstrates how to construct and sign URLs for use with the VDS-IS. This example script produces signatures compliant with the format used by the VDS-IS.

Depending on where the Python binary is installed, you may need to modify the first line of the script. The first line is only necessary if you plan to run the script as an executable. However, if you run the script using the Python interpreter, as documented in the “[Running a Python URL Signing Script](#)” section on page H-11, the first line is not required.



**Note** Sometimes media players append the port number to the URL. The port number is always removed when generating the URL signature.

```

#!/usr/local/bin/python
import md5
import hmac
import sha
import socket
import time
import sys
import optparse

def remove_port(url):
    """ Removes the port number from URL and then constructs the URL without port. """
    sep=":"
    arr=url.split(sep)
    url_no_port=arr[0]+sep
    if ( (len(arr)) == 3 ):
        url_no_port=url_no_port+arr[1]+"/"
        rem=arr[2].split("/",1)
        url_no_port=url_no_port+rem[1]
    return url_no_port
    else:
        return url

def sign_url(url,key):
    """ Signs url using key and returns the signed URL with the signature appended. """
    # Generate a MD5 hash of the key string (not the url)
    foo = md5.new(key)

    # Update the hash generated with the url string
    # This effectively means concatenating key and url and generating
    # a hash for the two
    foo.update(url)

    print "MD5 is used"
    # Get the digest in hex format (human readable)
    return url+foo.hexdigest()

def sign_url_sha1(url,key):
    """ Signs url using key and returns the signed URL with the signature appended. """
    foo = hmac.new(key,url,sha)
    print "SHA1 is used"
    return url+foo.hexdigest()

def remove_domain(url):
    """ Removes domain from the URL signature if set to 1, keep domain if set to 0. """

    sep="://"
    arr=url.split(sep)
    url = arr[1]
    sep="/"
    arr_1=url.split(sep,1)
    print "Remove domain"
    temp = arr[0] + "://" + arr_1[0]
    print "Remove domain PRINT:: " + temp

```

```

        arr_1[0] = temp
        print arr_1
        return arr_1

    def usage():
        """ Prints usage for the URL signing script. """

        print "Usage:"
        print "python cds-ims-urlsing.py <url> <client-ip> <expiry-delay-seconds>
<key-id-owner> <key-id-number> <key> <exclude-domain> <version>"
        print "Example:"
        print "python cds-ims-urlsing.py rtsp://abc.com/content/Apocalypto.mov
171.71.50.123 120 1 2 BubbaGump 1 ""or1or2

if __name__ == "__main__":
    """ Prints signed URL """

    parser = optparse.OptionParser()
    (options, args) = parser.parse_args()
    if len(sys.argv) < 8:
        usage()
        sys.exit(2)

    url = sys.argv[1]# URL
    client_ip = sys.argv[2]
    delay_seconds = sys.argv[3]# Number of seconds after which URL expires
    ko = sys.argv[4] # Key ID Owner
    kn = sys.argv[5] # Key ID Number
    key = sys.argv[6]# Key
    domain = sys.argv[7]# Exclude-domain config
    domain = int(domain)
    if ( len(args) == 7 ):
        version = ""
    else:
        version = sys.argv[8]
        version=int(version)

    # Set expiry time as current time (seconds since epoch) + delay
    et = time.time() + int(delay_seconds)
    expires = str(int(et))

    # Based on version we need to generate URL syntax for signing
    # By default v="" , which means sign URL with schema and no SIGV added. Uses md5
    # If v=0 , which means sign URL with schema and SIGV=0 added. Uses md5
    # If v=1 , which means sign URL with schema and SIGV=1 added. Uses sha1
    # If v=2 , which means sign URL without schema and SIGV=2 added. Uses sha1
    if ((version!="") & (version!=0) & (version!=1)):
        # python-2.5 is needed for partition. So will use split
        #schema,sep,url = url.partition(':')
        sep=":/"
        arr=url.split(sep)
        url = sep + arr[1]
        print url

        if url.find('?')==-1:
            url2 = url + "?"
        else:
            url2 = url + "&"

        url2 = remove_port(url2)

        if ((domain==1)):
            temp_arr = remove_domain(url2)

```

**■ URL Signing and Validating**

```

url2 = "/" + temp_arr[1]
print url2

# This string format is fixed and should not be modified.
# Note that we sign even the "&US=" part that will point to the signature
# If schema=1 then we need to append ver string as 0.
if (version==""):
    url2 = url2 +
"IS=0"&"ET="&expires+"&CIP="+client_ip+"&KO="+ko+"&KN="+kn+"&US=";
elif (version==0):
    url2 = url2 +
"IS=0"&"ET="&expires+"&CIP="+client_ip+"&KO="+ko+"&KN="+kn+"&US=";
elif (version==1):
    url2 = url2 +
"SIGV=1"&"IS=0"&"ET="&expires+"&CIP="+client_ip+"&KO="+ko+"&KN="+kn+"&US=";
elif (version==2):
    url2 = url2 +
"SIGV=2"&"IS=0"&"ET="&expires+"&CIP="+client_ip+"&KO="+ko+"&KN="+kn+"&US=";

# Based on the Version decide the sign Method to call
if ((version=="") | (version==0)):
    print url2
    url3 = sign_url(url2,key)

if ((version ==1) | (version==2)):
    print url2
    url3 = sign_url_sha1(url2,key)

#After we sign, if version=2 we add schema to signed URL
if ((version==2) & (domain!=1)):
    url3=arr[0]+url3
print url3

# Add the schema+domain after signature generation
if ((domain==1)):
    print temp_arr[0]
    if ((version==2)):
        url3 = arr[0] + temp_arr[0] + url3
    else:
        url3 = temp_arr[0] + url3
print url3

```

## Running a Python URL Signing Script

The example script can be used as follows:

```
python cds-ims-urlsing.py <url> <client-ip> <expiry-delay-seconds> <key-id-owner>
<key-id-number> <key> <exclude-domain> <version>
```

Syntax	Description
<i>url</i>	URL to sign.
<i>client-ip</i>	IP address of the client for which this URL is being signed, in dotted decimal format (A.B.C.D). The signed URL is rejected if sent from any other client when signature validation is enabled.
	<p><b>Note</b> The client-ip cannot be left blank or specified with empty quotes (""); it must be a valid IP address. If the client IP address is not to be considered in validating the URL, you can use any IP address as a place holder, and use the exclude validation option, which would not include the client IP address in the URL validation process. For the Web Engine and Flash Media Streaming, see the “Service Rule File for URL Validation and the Exclude-Validation Attribute” section on <a href="#">page E-32</a> for examples of the exclude-validation attribute. For Windows Media Streaming and Movie Streamer, see <a href="#">Table 4-13</a> on <a href="#">page 4-25</a> for configuring Service Rules on each SE.</p>
<i>expiry-delay-seconds</i>	Seconds (from now) when the URL expires. The request is rejected if the time period has passed when the URL is validated at the device. See the “Importance of Device Synchronization” section on <a href="#">page H-13</a> .
	<p><b>Note</b> The expiry-delay-seconds cannot be left blank or specified with empty quotes (""); it must be a number representing the expiration time for the URL. If the expiry time is not to be considered in validating the URL, you can use any number of seconds, and use the exclude validation option for the expiry time. For the Web Engine and Flash Media Streaming, see the “Service Rule File for URL Validation and the Exclude-Validation Attribute” section on <a href="#">page E-32</a> for examples of the exclude-validation attribute. For Windows Media Streaming and Movie Streamer, see <a href="#">Table 4-13</a> on <a href="#">page 4-25</a> for configuring Service Rules on each SE.</p>
<i>key-id-owner</i>	The first index into the key matrix. Valid entries are from 1 to 32.
<i>key-id-number</i>	The second index into the key matrix. Valid entries are from 1 to 16.
<i>key</i>	Shared secret key corresponding to this ordered pair ( <i>key-id-owner</i> , <i>key-id-number</i> ).

Syntax	Description
<i>exclude-domain</i>	If set to 1, exclude the domain from the URL signature. If set to 0, include the domain in the URL signature.  If the domain is excluded from the URL signature, then the domain must be excluded from the URL validation. To exclude the domain from URL validation, for the Web Engine and Flash Media Streaming, use the <b>exclude-domain</b> option for the <i>exclude-validate</i> attribute of the Rule_Validate element. For more information, see the “ <a href="#">Service Rule File Structure and Syntax</a> ” section on page E-4. To exclude the domain from the URL validation for Windows Media Streaming and Movie Streamer, use the <b>exclude domain-name</b> keyword for the <b>validate-url-signature</b> command. For more information, see the <a href="#">Table 4-13 on page 4-25</a> .
<i>version</i>	Hash algorithm used to generate the URL signature. The version number for the hash algorithm is as follows: <ul style="list-style-type: none"> <li>• 0 or none—To use MD5, enter zero (0) or do not enter a version number.</li> <li>• 1—To use SHA-1.</li> <li>• 2—To use SHA-1 and remove the protocol from the URL before signing.</li> </ul>

In addition to the above six variables, the current time is used to generate the URL signing, so even if the same values were used for the above variables, the signed URL would be different.



**Note** The client IP address and the content expiry are checked during validation based on the configuration of the Service Rules, which are either configured on each SE or configured by using the Service Rule XML file. For more information, see the “[Configuring the VDS-IS for URL Signing](#)” section on page H-3.

To use the URL signing script on the URL “rtsp://cisco.com/content/CiscoCDS.mov,” for the client IP address of 171.71.50.123, with an expiry delay of 120 seconds, a key ID owner of 1, a key ID number of 2, a key of kwnx90KGP, and the MD5 hash algorithm, enter the following:

```
python cds-ims-urlsing.py rtsp://cisco.com/content/CiscoCDS.mov 171.71.50.123 120 1 2
kwnx90KGP 0
```

The signed URL is the following:

```
rtsp://cisco.com/content/CiscoCDS.mov?IS=0&ET=1209422976&CIP=171.71.50.123&KO=1&KN=2&US=4f
b1c1adf1588fbe11cc6a04c6e69f35
```



**Note** The above signed URL is only an example. The hash algorithm generates a different message digest each time. For more information on the MD5 algorithm, see the IETF RFC 1321. For more information on the SHA-1 algorithm, see the IETF RFC 3174.

## URL Signing and Flash Media Streaming

When signing a URL for Flash Media Streaming VOD or Flash Media Streaming live streaming, the full URL for the request is used.

For the Flash Media Streaming interactive application, the Service Engine (acting as the Flash Media Streaming edge server proxy) routes the request to the origin server (which is the Flash Media Interactive Server) by way of the hierarchical path of Service Engines (each acting as proxy for the request). 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.

Requests for VOD and live streaming, and all the associated events, are received by the Service Engine and URL signature validation is performed in the PLAY event, which has the full URL, including the content name.

All Flash Media Streaming applications send CONNECT, PLAY, STOP, and DISCONNECT events. In the case of live streaming and VOD, all events are received by the Service Engine and the URL signature is validated in the PLAY event. In the case of interactive applications, only the CONNECT and DISCONNECT events are received by the Service Engine, all other events are proxied by the SE and processed on the origin server. The URL signature validation for interactive applications is performed on the CONNECT event, which does not include the content name.

[Table H-1](#) shows an example of each Flash Media Streaming delivery type, with the requested URL and the URL that is used in the URL Signing script.

**Table H-1      Flash Media Streaming URL Signing**

Delivery Type	Requested URL	URL Used in Signing
VOD	rtmp://fmsvod.com/vod/sample.flv	rtmp://fmsvod.com/vod/sample.flv
Live streaming	rtmp://livefms.com/live/livestream	rtmp://livefms.com/live/livestream
Interactive application	rtmp://fmsvod.com/myvod/sample.flv	rtmp://fmsvod.com/myvod

## Importance of Device Synchronization

URL expiry time validation relies on the assumption that the clocks are synchronized on the server running the signing application and the Service Engines validating the URL. Use of Network Time Protocol (NTP) on all devices, including the device running the signing application or script, is highly recommended.

It is not sufficient to merely have the same local times on two devices while their time zones differ.

For example, the following two devices are not synchronized:

- Device 1:
  - Local Time: 11:00:59 PM, October 12, 2008
  - Time Zone: PST
- Device 2:
  - Local Time: 11:00:59 PM, October 12, 2008
  - Time Zone: EST

The following two devices are synchronized:

- Device 1:
  - Local Time: 11:00:59 AM, October 12, 2008

- Time Zone: PST
- Device 2:
  - Local Time: 2:00:59 PM, October 12, 2008
  - Time Zone: EST

## Understanding the Signing Procedure

To customize the URL signing script for your portal, or to write your own signing application in the platform and language of your choice, and still be able to validate URLs within the VDS-IS, follow the steps explained in this section.

The URL signing script performs these steps when processing an unsigned URL:

1. Reads the version information from the script argument and removes the protocol from the URL if the version equals 2.
2. Checks if the URL already contains a query string.
  - If the URL does not contain a query string, appends a question mark (?).
  - If the URL does contain a query string, appends an ampersand (&).
3. Removes the port number in the URL, if one exists.
4. Appends the string **IS=0**. This string is for legacy support with some VDS-IS components that use both internal (within VDS-IS) and external (**portal**) signing mechanisms.
5. Appends the string **&ET=**.
6. Gets the current time in seconds since epoch (as an integer). Adds the expiry time in seconds as an integer and appends this integer.
7. Appends the string **&CIP=**.
8. Appends the requesting client IP address, using dotted decimal format.
9. Appends the string **&KO=**.
10. Appends the key ID owner corresponding to the key being used.
11. Appends the string **&KN=**.
12. Appends the key ID number corresponding to the key being used.
13. Appends the string **&US=**.
14. Stores this as url2; for example:  
**“rtsp://cisco.com/content/CiscoCDS.mov?IS=0&ET=1209422976&CIP=171.71.50.123&KO=1&KN=2&US=”**
15. Generates an MD5 hash of the key being used.
16. Updates the generated hash with url2.
17. Converts the hash to its equivalent human readable hex digest; for example:  
**4fb1c1adf1588fbe11cc6a04c6e69f35**
18. Appends the hex digest to url2. The URL signing is complete.

## Public Key URL Signing for Asymmetric Keys

Asymmetric keys always have a key pair made up of a public key and private key. The private key is used for signing and the public key is used for validation.

The public key URL signing supports Elliptic Curve (EC) keys and uses EC Digital Signature Algorithm (DSA), which is the EC equivalent of DSA for signature generation and signature validation.

Elliptic Curve Cryptography (ECC) has the following main advantages:

- Key size is small while still offering good security
- Key is easy to store
- Computation is faster than DSA or RSA

The signed URL of EC-DSA contains some clear text data (for example, client IP [CIP], expiry time [ET], and the US=DSA r and s values). For transport security, the VDS-IS software takes these tag values, converts them into hexadecimal values, then encrypts them using American Encryption Standard (AES) Counter (CTR) mode and 128-bits key size when the **url-signature** command **symmetric-key** option is configured by the user. The encrypted output is attached to the URL as base64 encoded data. Both hexadecimal and Base64 conversions produce URL-safe values, but Base64 produces smaller output, which is why AES encrypted output is converted to Base64.

## How Public Key URL Signing Works with VDS-IS

You can generate a pair of EC keys and write each key (public and private) into separate files (a public key file and a private key file) by using the Privacy Enhanced Mail (PEM) format. The **url-signature** command has keyword options that provide a way to upload these files and associate them to a particular key owner and key number. If you want secure transmission of the CIP, ET, and US tag values, you can use the **symmetric-key** option of the **url-signature** command., which uses AES to encrypt the CIP, ET, and US tag values. The CDSM GUI offers the same options for uploading the files and secure transmission. See the “[Configuring URL Signing Key](#)” section on page 4-27 for more information.

The URL can be signed externally using the C binary. The signed URL is then sent to the VDS-IS for signature validation. The VDS-IS validates the signed URL by using the key owner (KO) and key number (KN) to look up the URL signature.

The **url-signature** command and the URL Signing page in the CDSM GUI (“[Configuring URL Signing Key](#)” section on page 4-27) offer the ability to generate the URL signature for symmetric keys and asymmetric keys, as well as validate them. Additionally, URL Signing can be configured on a per-Delivery Service basis by using the Service Rule XML file (“[URL Signing Key in the Service Rule File](#)” section on page E-18).

### url-signature Command

The **url-signature** command creates a symmetric key or asymmetric key for the URL signature.

```
url-signature key-id-owner key-id-owner key-id-number key-id-number {key key | public-key  
public-key [private-key private-key [symmetric-key] | symmetric-key]}
```

Syntax	Description
<b>key-id-owner</b>	Configures the owner for this key.
<i>key-id-owner</i>	Specifies the ID for the owner of this key. Valid entries are from 1 to 32.
<b>key-id-number</b>	Configures the ID number for this key.

## ■ URL Signing and Validating

<i>key-id-number</i>	Specifies the ID for the number of this key. Valid entries are from 1 to 32.
<b>key</b>	Configures the symmetric encryption key for signing a URL.
<i>key</i>	Specifies the encryption key. The maximum number of characters is 16. Spaces are not allowed.
<b>public-key</b>	Configures the public key for the specified key owner (KO) and key number (KN).
<i>public-key</i>	Specifies the public key.
<b>private-key</b>	Optional. Configures the private key for the specified KO and KN.
<i>private-key</i>	Specifies the private key.
<b>symmetric-key</b>	Optional. Uses AES to further encrypt the CIP, ET, and US tag values by using the symmetric-key. The length of the AES key is 16 bytes or 128 bits, which is 16 characters.

Following is an example of generating and encrypting the public key and private key using the **url-signature** command:

```
(config)# url-signature key-id-owner 1 key-id-number 10 public-key http://1.1.1.1/ec_pub_key private-key
http://1.1.1.1/ec_pub_key symmetric-key
```

## URL Signing C Program

To use the C binary to generate the signed URL using the private key, follow these steps:

---

**Step 1** Get the following information from the client:

- URL
- Expiry time
- Client IP address
- Private key file
- Key owner
- Key number
- Symmetric key (AES encryption)



**Note** The client-ip cannot be left blank or specified with empty quotes (""); it must be a valid IP address. If the client IP address is not to be considered in validating the URL, you can use any IP address as a place holder, and use the exclude validation option, which would not include the client IP address in the URL validation process. For the Web Engine, Flash Media Streaming, and Windows Media Streaming, see the [“Service Rule File for URL Validation and the Exclude-Validation Attribute” section on page E-32](#) for examples of the exclude-validation attribute. For Movie Streamer, see [Table 4-13 on page 4-25](#) for configuring Service Rules on each SE.

**Note**

The expiry-delay-seconds cannot be left blank or specified with empty quotes (""); it must be a number representing the expiration time for the URL. If the expiry time is not to be considered in validating the URL, you can use any number of seconds, and use the exclude validation option for the expiry time. For the Web Engine, Flash Media Streaming, and Windows Media Streaming, see the [“Service Rule File for URL Validation and the Exclude-Validation Attribute” section on page E-32](#) for examples of the exclude-validation attribute. For Movie Streamer, see [Table 4-13 on page 4-25](#) for configuring Service Rules on each SE.

- Step 2** Construct the URL to be signed by removing the schema (the protocol of the URL, for example, HTTP) from the URL.
- Step 3** Get the length of the constructed URL and add a tag “LENTOSIGN” before the US tag.
- Step 4** Create a digest of the URL with the LENTOSIGN tag using SHA-1 without a key.
- Step 5** Sign this digest with an EC private key.
- Step 6** The signature contains two values, *r* and *s*. Convert them to Hexadecimal and add them to the signed URL.
- Step 7** If an AES key is configured, convert the CIP, ET, and US tag values to hexadecimal values, and encrypt them using AES CTR 128 mode. The Initialization Vector (IV) used is 64 bits. The IV is encoded to base64 and added to the URL. After appending the IV to the URL , then append the encrypted data using AES CTR 128. This encrypted data should be encoded to base64 before adding it to URL.

Following is some sample output from C binary:

```
# ./public_key
The usage is ./public_key <url> <client-ip> <expiry-delay-seconds> <key-id-owner>
<key-id-number> <private_key_file> <Symmetric-Key>
The number of arguments is less than 8

# ./public_key rtsp://www.cisco.com/my.wmv 1.1.1.1 20000 1 2 test_priv ciscociscociscoc
Url : rtsp://www.cisco.com/my.wmv , Ko : 1 , KN : 2 Expiry_time : 20000
The Private Key read from file is : -----BEGIN EC PRIVATE KEY-----
MIIBUQIBAQQgNu8C5npnuJPzS+vUDLzbvYHebXyd2fqI71cFIPky+uggeMwgeAC
AQEWlAYHKoZIzj0BAQIhAP///8AAABAAAAAAA/AAAAAAA/AAAAAAA/AAAAAAA/AAAAAAA/
MEQEIP///8AAABAAAAAAA/AAAAAAA/AAAAAAA/AAAAAAA/8BCBaxjXYqjqT57Pr
vVV2mIa8ZR0GsMxTsPY7zjw+J9JgSwRBBGsX0fLhLEJH+Lzm5WOkQPJ3A32BLesr
oPSheOUXYmMKWT+NC4v4af5u05+tKfA+eFivOM1drMV7Oy7ZAaDe/UfUCIQD///
AAAAAP///vOb6racXnoTzucrC/GM1UQIBAAFEA0IAHZ7vJFy6si5SOY1E
40aByIjsFYuZ9eVuLyolpyhnX0GINMfkLoJBT0KhJfah5zNuKRSi6V8NtUpaUc28
BYKqx6A=
-----END EC PRIVATE KEY-----

The ET time value is : 1248690812
The schema removed URL is : :://www.cisco.com/my.wmv
The URL to calculate LENTOSIGN is :
:://www.cisco.com/my.wmv?SIGV=3&IS=0&CIP=1.1.1.1&ET=1248690812&KO=1&KN=2&US=
The URL LENTOSIGN value is : 75
The URL ready for sha1 sign without Key :
:://www.cisco.com/my.wmv?SIGV=3&IS=0&CIP=1.1.1.1&ET=1248690812&KO=1&KN=2&LENTOSIGN=79&US=
The ECDSA Signed URL is :
rtsp://www.cisco.com/my.wmv?SIGV=3&IS=0&CIP=1.1.1.1&ET=1248690812&KO=1&KN=2&US=DSA=r:CFB03
EDB33810AB6C79EE3C47FBDB86D227D702F25F66C01CF03F59F1E005668D:s:57ED0E8DF7E786C87E39177DD339
8A7FB010E6A4C0DC8AA71331A929A29EA24E
The base64 encoded IV is : cXgS7eo+sHc=
The ET value to be converted to Hex is : 1248690812The Hex converted ET string is :
0c304500080c
```

## ■ URL Signing and Validating

```

The IP to be converted to Hex is : 1.1.1.1Hex representation of IP Value is : 01010101
The length of SIG->r is : 64
The length of SIG->r is : 32
The constructed Hex string after adding SIG->r Tag representation :
01060c304500080c0204010101010332CFB03EDB33810AB6C79EE3C47FBD86D227D702F25F66C01CF03F59F1E0
05668D
The length of SIG->s is : 64
The length of SIG->s is : 32
The data that will be encrypted is :
01060c304500080c0204010101010332CFB03EDB33810AB6C79EE3C47FBD86D227D702F25F66C01CF03F59F1E0
05668D043257ED0E8DF7E786C87E39177DD3398A7FB010E6A4C0DC8AA71331A929A29EA24E
The AES Encrypted URL is :
rtsp://www.cisco.com/my.wmv?SIGV=3&IS=0&KO=1&KN=2&cXgS7eo+sHc=X+HOeJ6yKmUmmzLObphXZ98ttyj7
BaAeQF1hCaYBxwHgswiNAW+Uj+IHBLojKgxixCXULiPBmawF1czVKrvVmpvA8OoQ5ujJzpjYXeLLBGGSs3g==
```

## C Program for URL Signing

The pseudo code for signature generation has the following tasks:

- 
- Step 1** Make sure the C program accepts the following values as command line arguments to generate the signed URL:
    - URL
    - Client\_IP
    - Expiry\_time
    - KO
    - KN
    - Private Key file in PEM format
    - Symmetric Key (for AES Encryption)
  - Step 2** After reading the arguments, check if the Private Key file can be read. If yes , run **fread** to read all the data .
  - Step 3** The URL given as the input argument to the program should then be passed to the function that can remove the schema (the protocol, for example, HTTP) from the URL. For example, <http://www.cisco.com/index.html> should be changed to <://www.cisco.com/index.html>.
  - Step 4** Construct the URL with all the sign tags as follows:

```
snprintf(url_lentoadd , URL_MAX,
        "%s%c" "%s&" "%s" "&%s=%s" "&%s=%s" "&%s=%s" "&%s=%s" "&%s=%s",
        url, '?',
        sigv, "IS=0",
        "CIP", ip,
        "ET", cur_time,
        "KO", ko,
        "KN", kn,
        "US" );
```

An example of the output follows:

```
//www.cisco.com/index.html?SIGV=3&IS=0&CIP=1.1.1.1&ET=123456789&KO=1&KN=3&US=
```

In the above call **snprintf** , we construct the URL as above. The **cur\_time** is calculated as **Epoch\_time + expiry time** .

- Step 5** Calculate the length of the URL formed in [Step 4](#).

For example, the length of URL

`://www.cisco.com/index.html?SIGV=3&IS=0&CIP=1.1.1.1&ET=123456789&KO=1&KN=3&US` is 78.

**Step 6** Reconstruct the URL again with the new Tag LENTOSIGN added before the US tag as follows:

```
snprintf(url_to_sign, URL_MAX,
        "%s%c" "%s&" "%s" "&%s=%s" "&%s=%s" "&%s=%s" "&%s=%s" "&%s=%d" "&%s=" ,
        url_without_schema,(strchr(url, '?')) ? '&' : '?',
        sigv,"IS=0",
        "CIP",ip,
        "ET",cur_time,
        "KO",ko,
        "KN",kn,
        "LENTOSIGN",len_to_add,
        "US");
```

An example of the output follows:

`://www.cisco.com/index.html?SIGV=3&IS=0&CIP=1.1.1.1&ET=123456789&KO=1&KN=3&LENTOSIGN=82&US=`



**Note** The value of LENTOSIGN is taken from [Step 5](#). Also the URL does not have the schema (protocol).

**Step 7** The URL is ready to be signed using SHA-1 without a key. An example of a URL ready for SHA-1 without a key follows:

`://www.cisco.com/index.html?SIGV=3&IS=0&CIP=1.1.1.1&ET=123456789&KO=1&KN=3&LENTOSIGN=82&US=`

The following APIs are used to sign the URL:

```
create_digest(sign,url_to_sign);
void create_digest(char *digest,char *data)
{
    memset(digest,0,sizeof(digest));
    int md_len;
    unsigned char digest1[20];
    EVP_MD_CTX md_ctx;
    EVP_MD_CTX_init(&md_ctx);
    EVP_DigestInit_ex(&md_ctx, EVP_ecdsa(),NULL);
    EVP_DigestUpdate(&md_ctx,data,strlen(data));
    EVP_DigestFinal_ex(&md_ctx,digest,&md_len);
}
```

**Step 8** The private key is read from the file and EC\_KEY is created using the following APIs:

```
EC_KEY *eckey=NULL;
ECDSA_SIG *sig=NULL;
BIO *out_priv=NULL;

out_priv=BIO_new_mem_buf(private_key,strlen(private_key));
eckey=(EC_KEY *)PEM_read_bio_ECPPrivateKey(out_priv,NULL,NULL,NULL);
```

**Step 9** The EC-DSA signature is created using the EC\_KEY on the digest that was created in [Step 7](#).

```
sig=ECDSA_do_sign(sign,20,eckey);
```

If the signature is successful, the `sig` parameter contains r and s values. Extract the r and s values using the following commands:

```
BN_bn2hex(sig->r)
BN_bn2hex(sig->s)
```

**Step 10** Add these signature values to the URL generated in [Step 4](#).

```
strcat(url_lentoadd, "DSA=r:");
strcat(url_lentoadd, BN_bn2hex(sig->r));
strcat(url_lentoadd, ":s:");
strcat(url_lentoadd, BN_bn2hex(sig->s));
```

An example of the final EC-DSA signed URL follows:

```
http://www.cisco.com/index.html?SIGV=3&IS=0&CIP=1.1.1.1&ET=123456789&KO=1&KN=3&US=DSA=r:CF
B03EDB33810AB6C79EE3C47FBD86D227D702F25F66C01CF03F59F1E005668D:s:57ED0E8DF7E786C87E39177DD
3398A7FB010E6A4C0DC8AA71331A929A29EA24E
```

**Step 11** If transport security needs to be applied to the Tag values (CIP, ET, and US), use AES CTR 128 encryption. Convert them to hexadecimal format. Following is an example:

#### **ET : 01 length hexadecimal\_value of ET**

ET is 01 length hexadecimal (1248690812). The resulting value is: 01 06 0c304500080c, which equals 01060c304500080c. The ET value is converted to hexadecimal by taking two digits at a time from the original ET, which in the example is 1248690812. Following are each two-digit conversion:

- 12 = 0c
- 48 = 30
- 69 = 45
- 08 = 00 08
- 12 = 0c

Each hexadecimal is four bits. The length is calculated based on the resulting values from the hexadecimal conversion. In the example, there are six 8-bit lengths: 0c 30 45 00 08 0c.

#### **CIP : 02 length hexadecimal (IP)**

CIP is 02 length hexadecimal (1.1.1.1). The resulting value is : 02 04 01010101, which equals 020401010101.

#### **US : 03 length sig->r**

US is : 03 length ( CFB03EDB33810AB6C79EE3C47FBD86D227D702F25F66C01CF03F59F1E005668D). The resulting value will be : 03 32 CFB03EDB33810AB6C79EE3C47FBD86D227D702F25F66C01CF03F59F1E005668D, which equals 0332CFB03EDB33810AB6C79EE3C47FBD86D227D702F25F66C01CF03F59F1E005668D.

#### **US : 04 length sig->s**

US is: 04 length (sig->s). The resulting value is: 04 3257ED0E8DF7E786C87E39177DD3398A7FB010E6A4C0DC8AA71331A929A29EA24E, which is equal to 043257ED0E8DF7E786C87E39177DD3398A7FB010E6A4C0DC8AA71331A929A29EA24E.

The AES Key should be exactly16 bytes in length. It cannot be greater than 16 bytes or less than 16 bytes .

**Step 12** Once the ET , CIP and US Tag values have been constructed in hexadecimal, they need to put together to send them to AES CTR encrypt API .

The values from [Step 11](#) are the following:

```
01060c304500080c + 020401010101 +
0332CFB03EDB33810AB6C79EE3C47FBD86D227D702F25F66C01CF03F59F1E005668D +
043257ED0E8DF7E786C87E39177DD3398A7FB010E6A4C0DC8AA71331A929A29EA24E
```

The data that is encrypted using AES CTR 128 is the following:

```
01060c304500080c0204010101010332CFB03EDB33810AB6C79EE3C47FBD86D227D702F25F66C01CF03F59F1E0
05668D043257ED0E8DF7E786C87E39177DD3398A7FB010E6A4C0DC8AA71331A929A29EA24E
```

The data that is encrypted using AES CTR is converted to char \* , so the length is 82 bytes.

- Step 13** Before calling the APIs to perform the AES CTR encryption, the IV needs to be generated. The IV generated is 64 bits in length.

```
RAND_bytes(iv, 8);
```

With the IV that is generated and the resultant data from [Step 12](#), use the following APIs to encrypt the data using AES CTR mode.

```
AES_set_encrypt_key(sym_key,AES_BLOCK_SIZE*8,&keys);
AES_ctr128_encrypt(); //Need to pass all the arguments
```

- Step 14** Construct the AES Encrypted URL over EC-DSA signature as follows :

```
snprintf(final_aes,URL_MAX,
        "%s%c" " %s" "&%s=%s" "&%s=%s" "&%s=%s" "&%s=%s" "%s",
        url,(strchr(url, '?')) ? '&' : '?',
        sigv,
        "IS", "0",
        "KO", ko,
        "KN", kn,
        "US",
        base64_iv_p,
        base64_encode);
```



**Note** The IV generated is converted to Base64 format. It is attached to URL after the “US=” tag. The AES CTR encryption output is converted to Base64 format and appended to the URL after adding IV.

For example, if the Base64 encoded IV is : cXgS7eo+sHc=, and the AES CTR encryption output in Base64 format is :

```
X+HOeJ6yKmUmmzLObphXZ98tjy7BaAeQF1hCaYBxwHgswiNAW+Uj+IHBLojKgxiCXULiPBma
wF1czVKrvVmpvA8OoQ5ujJzpjYXeLLBGGSs3g==
```

The final AES encrypted URL is as follows:

```
http://www.cisco.com/index.html?SIGV=3&IS=0&KO=1&KN=3&US=
```

- Step 15** Add the IV in Base64 format to the URL.

```
http://www.cisco.com/index.html?SIGV=3&IS=0&KO=1&KN=3&US=cXgS7eo+sHc=
```

- Step 16** Finally, append the AES encryption output in Base64 format.

```
http://www.cisco.com/index.html?SIGV=3&IS=0&KO=1&KN=3&US=cXgS7eo+sHc=
X+HOeJ6yKmUmmzLObphXZ98tjy7BaAeQF1hCaYBxwHgswiNAW+Uj+IHBLojKgxiCXULiPBmawF1czVKrvVmpvA8Oo
Q5ujJzpjYXeLLBGGSs3g==
```

These are the detailed steps that are used in generating a signed URL. This can be implemented completely using a C program.

■ URL Signing and Validating



## CLI Commands

This appendix covers the following topics:

- [Multi-Port Support, page I-1](#)
- [Configuring Port Channel, page I-6](#)
- [Configuring Last-Resort Routing, page I-11](#)
- [Configuring Standby Interfaces, page I-12](#)

## Multi-Port Support

Multi-port support allows the configuration of multiple interfaces, each with a different IP address, all used for streaming traffic. An interface could be a gigabit Ethernet channel, a port channel, or a standby group. Multi-port support allows for utilization of the total bandwidth available in the platform and is introduced solely to support the all the platforms.

The main reason Multi-port support is added is because a switch has a hard limit of 8 interfaces that can be grouped into a port-channel, so to fully use all 12 gigabit Ethernet interfaces, multi-port support was added.

### Redirection with Proximity Engine

If an SE is configured with more than one streaming interface IP address and the SR uses proximity-based routing, the Proximity Engine uses the first valid IP address when performing the proximity check. Proximity-based routing is used to select the closest Service Engine for a specified client IP address, and it is assumed the client has the same proximity to all IP addresses of the SE.

The first valid streaming interface is the first interface displayed in the **show run** command. The order in which the streaming interfaces display depends on the order of configuration, as well as the history of the configuration modifications (for example, if a streaming interface was deleted and then added again). It is not possible to guarantee a certain display order of the streaming interfaces; therefore, it is not possible to guarantee that a certain streaming interface IP address is used for the proximity check.

### Configuring Multi-Port Support

Multi-port support allows for configuring a list of streaming interfaces. If there are 14 gigabit Ethernet channels in the system, then there could be a maximum of 14 streaming interfaces, each with their own unique IP address. This example is for the CDE220-2G2, which has 10 gigabit Ethernet interfaces. The CDE110 and CDE205 have 2 gigabit Ethernet interfaces and the platform has 14 gigabit Ethernet interfaces.

The following commands can be used to add a streaming interface.

**Multi-Port Support**

```

SE-CDE220-1(config)# streaming-interface portChannel 1
SE-CDE220-1# show run
    ! CDS version 2.5.0
    !
    device mode service-engine
    !
    !
    hostname SE-CDE220-1
    !
    primary-interface PortChannel 1
    !
    interface Standby 1
        IP address 1.2.3.4 255.255.255.0
        exit
    interface Standby 3
        IP address 4.5.6.7 255.255.255.0
        exit
    !
    interface PortChannel 1
        IP address 7.9.0.3 255.255.0.0
        exit
    !
    interface GigabitEthernet 1/0
        shutdown
        exit
    interface GigabitEthernet 2/0
        standby 3
        exit
    interface GigabitEthernet 3/0
        channel-group 1
        exit
    interface GigabitEthernet 4/0
        channel-group 1
        exit
    interface GigabitEthernet 5/0
        channel-group 1
        exit
    interface GigabitEthernet 6/0
        channel-group 1
        exit
    interface GigabitEthernet 7/0
        shutdown
        exit
    interface GigabitEthernet 8/0
        shutdown
        exit
    interface GigabitEthernet 9/0
        shutdown
        exit
    interface GigabitEthernet 10/0
        shutdown
        exit
    !
    streaming-interface PortChannel 1
    streaming-interface GigabitEthernet 8/0

```

Use the **no** form of the command to delete an interface. The following example shows the deletion of a streaming interface:

```

SE-CDE220-1(config)# no streaming-interface gigabitEthernet 8/0
SE-CDE220-1# show run
    ! CDS version 3.0.0
    !
    device mode service-engine

```

```
!
!
hostname SE-CDE220-1
!
primary-interface PortChannel 1
!
interface Standby 1
  IP address 1.2.3.4 255.255.255.0
  exit
interface Standby 3
  IP address 4.5.6.7 255.255.255.0
  exit
!
interface PortChannel 1
  IP address 7.9.0.3 255.255.0.0
  exit
!
interface GigabitEthernet 1/0
  shutdown
  exit
interface GigabitEthernet 2/0
  standby 3
  exit
interface GigabitEthernet 3/0
  channel-group 1
  exit
interface GigabitEthernet 4/0
  channel-group 1
  exit
interface GigabitEthernet 5/0
  channel-group 1
  exit
interface GigabitEthernet 6/0
  channel-group 1
  exit
interface GigabitEthernet 7/0
  shutdown
  exit
interface GigabitEthernet 8/0
  shutdown
  exit
interface GigabitEthernet 9/0
  shutdown
  exit
interface GigabitEthernet 10/0
  shutdown
  exit
!
streaming-interface PortChannel 1

SE-CDE220-1(config)# no streaming-interface gigabitEthernet 8/0
No Configuration exists to delete
```

### Multiple IP addresses and Default Gateway Example

The following example shows how to configure the streaming interfaces on a CDE220-2S3i with multiple IP addresses and a default gateway, plus adding the necessary IP routes.

**Note**

If the CDE220-2S3i has multiple IP addresses and is configured in a private network address space, then each internal IP address needs an external NAT entry defined on the main core router or switch.

The IP default gateway can only be configured when the physical network connection and VLAN is configured and active on the switch or router. If the VLAN is not ready when you configure the IP default gateway, you get an error message stating that the default gateway address is invalid.

This example consists of the following steps:

---

**Step 1** Creating a port channel.

```
CC1-2S3-4(config)# interface portChannel 1
CC1-2S3-4(config-if)# ip add 8.4.0.8 255.255.0.0
CC1-2S3-4(config-if)# exit
CC1-2S3-4(config)# interface portChannel 2
CC1-2S3-4(config-if)# ip add 6.22.1.2 255.255.255.0
CC1-2S3-4(config-if)# exit
CC1-2S3-4(config)# interface portChannel 3
CC1-2S3-4(config-if)# ip add 6.23.1.2 255.255.255.0
CC1-2S3-4(config-if)# exit
CC1-2S3-4(config)#

```

**Step 2** Creating an IP default gateway. This step cannot be done unless the physical network connection and switch side VLAN is configured first.

```
CC1-2S3-4(config)# ip default-gateway 8.4.0.1 6.22.1.1 6.23.1.1
CC1-2S3-4(config)#

```

The **show ip route** command displays the following:

```
CC1-2S3-4# show ip route
Destination      Gateway          Netmask
-----  -----
6.22.1.2        0.0.0.0         255.255.255.255
8.4.0.8          0.0.0.0         255.255.255.255
6.23.1.2        0.0.0.0         255.255.255.255
6.23.1.0        0.0.0.0         255.255.255.0
6.22.1.0        0.0.0.0         255.255.255.0
8.4.0.0          0.0.0.0         255.255.0.0
0.0.0.0          8.4.0.1          0.0.0.0
0.0.0.0          6.22.1.1         0.0.0.0
0.0.0.0          6.23.1.1         0.0.0.0

Number of route cache entries: 14
```

```
Table for interface 8.4.0.8 :
0.0.0.0          0.0.0.0         8.4.0.1
```

```
Table for interface 6.22.1.2 :
0.0.0.0          0.0.0.0         6.22.1.1
```

```
Table for interface 6.23.1.2 :
0.0.0.0          0.0.0.0         6.23.1.1
```

**Step 3** Adding gigabit Ethernet interfaces into the port channel.

```
CC1-2S3-4(config)# interface gigabitEthernet 3/0 channel-group 1
CC1-2S3-4(config)# interface gigabitEthernet 4/0 channel-group 1
CC1-2S3-4(config)# interface gigabitEthernet 5/0 channel-group 1
CC1-2S3-4(config)# interface gigabitEthernet 6/0 channel-group 1
CC1-2S3-4(config)# interface gigabitEthernet 7/0 channel-group 2
CC1-2S3-4(config)# interface gigabitEthernet 8/0 channel-group 2
CC1-2S3-4(config)# interface gigabitEthernet 9/0 channel-group 2
CC1-2S3-4(config)# interface gigabitEthernet 10/0 channel-group 2
CC1-2S3-4(config)# interface gigabitEthernet 11/0 channel-group 3
CC1-2S3-4(config)# interface gigabitEthernet 12/0 channel-group 3
```

```
CC1-2S3-4(config)# interface gigabitEthernet 13/0 channel-group 3
CC1-2S3-4(config)# interface gigabitEthernet 14/0 channel-group 3
```

**Step 4** Creating a streaming interface for the port channel.

```
CC1-2S3-4(config)# streaming-interface portchannel 1
CC1-2S3-4(config)# streaming-interface portchannel 2
CC1-2S3-4(config)# streaming-interface portchannel 3
```

---

### Service Router Monitoring

The Service Router now associates multiple IP addresses to a particular SE. From the SR, use the following command to check the list of IP addresses of the SE.

```
SR# show service-router services sename SE-CDE220-1
```

```
-- Services Status Of SE: SE-CDE220-1-
IP address : 7.9.0.7
IP address : 2.2.2.2
Aliveness : up
Critical Service(s) : Running
Service WEB
    Running : Yes
    Threshold : Not reached

Service WMT
    Running : Yes
    Threshold : Not reached

Service MS
    Running : No

Service FMS
    Running : Yes
    Threshold : Not reached
```

The SEs send keepalives to the SR at stipulated intervals. In the keepalives, the list of the IP addresses associated with the particular SE are also sent. Along with the list of interfaces and their corresponding IP addresses, the network interface card (NIC) utilization for each of these interfaces is also sent. If a particular interface is not active, that particular IP is not sent in the keepalive. If no streaming interfaces are configured, then no keepalives are sent to the SR.

The SR chooses an SE interface with the least NIC utilization and redirects the client request to that particular IP address. If the NIC utilization of all the interfaces are equal, then the interface for streaming is chosen at random. The NIC utilization is the maximum of the average ingress bandwidth percentage and the average egress bandwidth percentage of the interface.

The NIC utilization for each of interface is tracked and check if the threshold has been exceeded. The utilization values monitored on the service monitor are sent to the SR. The NIC sampling interval and the number of samples can be configured using the CDSM. The NIC threshold of an SE is reached only when the thresholds of all the streaming interfaces have been reached.

The current NIC status can be checked using the following command:

```
SE-CDE220-1# show service-router service-monitor
```

```
NIC
Interface : PortChannel 1
Average BW In : 0%
Average BW Out : 0%
Threshold : Not reached
```

## Configuring Port Channel

```

Interface          : Standby 2
Average BW In    : 0%
Average BW Out   : 0%
Threshold        : Not reached

```

# Configuring Port Channel

To configure an EtherChannel, you use the **PortChannel** interface configuration command. Port Channel, also known as EtherChannel, supports the grouping of up to eight same-speed network interfaces into one virtual interface. EtherChannel also provides interoperability with Cisco routers, switches, and other networking devices or hosts supporting EtherChannel; load balancing; and automatic failure detection and recovery based on each interface's current link status.



- Note** To achieve the best throughput, we recommend you configure a port channel for the eight gigabit Ethernet ports on the line card. Up to eight gigabit Ethernet interfaces can be put into the same port channel.

# Redundant Dedicated Management Ports

On a CDE220-2G2 configured as an SE or SR, there are ten gigabit Ethernet ports. All the ports can be used for delivery traffic such as RTSP, as well as system management traffic to communicate with other VDS-IS devices such as the CDSM. To prevent all the bandwidth being used by delivery traffic, a dedicated management port setup is often recommended.

In case of physical failure on a single port, channel bonding configuration of multiple gigabit Ethernet ports is also recommended for both delivery traffic and management traffic.



- Note** A port channel configured with a default gateway is only for delivery traffic. Delivery traffic places highest bandwidth demand on the VDS-IS network. A port channel configured as the primary interface carries delivery traffic.



- Note** If an EtherChannel (also known as port channel) is used between the upstream router or switch and the SE for streaming real-time data, the EtherChannel load balance algorithms on the upstream switch or router and the SE should be configured as “src-ip” and “dst-ip” respectively. Using this configuration ensures session stickiness and general balanced load-distribution based on clients' IP addresses. Also, distribute your client IP address space across multiple subnets so that the load-balancing algorithm is effective in spreading the traffic among multiple ports.

On a CDE220-2G2, two gigabit Ethernet ports on the motherboard (GigabitEthernet 1/0 and 2/0) can be bundled for the management port channel, and eight gigabit Ethernet ports (GigabitEthernet 3/0 to 10/0) on the NICs can be bundled for the traffic port channel for maximum throughput. For more redundancy, you can configure two channel groups of four interfaces each (3/0 to 6/0 and 7/0 to 10/0) that are standbys for each other.

## Configuring Redundant Management Ports

To configure redundant dedicated management ports on a CDE220 using the CLI, follow these steps:

- 
- Step 1** Configure two port channels with different subnets for each one.

```
SE(config)# interface PortChannel 1
SE(config-if)# IP address 3.1.7.73 255.255.255.0
SE(config-if)# exit
SE(config)# interface PortChannel 2
SE(config-if)# IP address 3.1.8.200 255.255.255.0
SE(config-if)# exit
```

- Step 2** Assign the interfaces to the two port channels. PortChannel 1 has four gigabit Ethernet interfaces for application traffic, and PortChannel 2 has two gigabit Ethernet interfaces for management traffic.

```
SE(config)# interface GigabitEthernet 1/0
SE(config-if)# channel-group 2
SE(config-if)# exit
SE(config)# interface GigabitEthernet 2/0
SE(config-if)# channel-group 2
SE(config-if)# exit
SE(config)# interface GigabitEthernet 3/0
SE(config-if)# channel-group 1
SE(config-if)# exit
SE(config)# interface GigabitEthernet 4/0
SE(config-if)# channel-group 1
SE(config-if)# exit
SE(config)# interface GigabitEthernet 5/0
SE(config-if)# channel-group 1
SE(config-if)# exit
SE(config)# interface GigabitEthernet 6/0
SE(config-if)# channel-group 1
SE(config-if)# exit
```



- Note** The port channel carrying delivery traffic should always be configured as channel-group 1 and set as the primary interface.



- Note** Whenever the IP address of the primary interface is changed, the DNS server needs to be restarted.

- 
- Step 3** Configure the delivery port channel as the primary interface.

```
SE(config)# primary-interface PortChannel 1
```

- Step 4** Configure a default gateway for the delivery traffic.

```
SE(config)# ip default-gateway 3.1.7.1
```

- Step 5** Set the load balancing algorithm to the destination IP address.

```
SE(config)# port-channel load-balance dst-ip
```

- Step 6** Configure a static route to the CDSM (4.0.5.5) to specify that all management traffic goes through this interface.

```
SE(config)# ip route 4.0.5.5 255.255.255.255 3.1.8.1
```

## Configuring Port Channel

- Step 7** Configure the port channel and VLANs on the switch that the SE is directly connected to.

```
SW3750(config)# interface Port-channel1
SW3750(config-if)# switchport access vlan 201
SW3750(config-if)# exit
SW3750(config)# interface Port-channel2
SW3750(config-if)# switchport access vlan 202
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/1
SW3750(config-if)# description Connected to portchannel2
SW3750(config-if)# switchport access vlan 202
SW3750(config-if)# channel-group 2 mode on
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/2
SW3750(config-if)# description Connected to portchannel2
SW3750(config-if)# switchport access vlan 202
SW3750(config-if)# channel-group 2 mode on
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/3
SW3750(config-if)# description connected to portchannel1
SW3750(config-if)# switchport access vlan 201
SW3750(config-if)# channel-group 1 mode on
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/4
SW3750(config)-if# description connected to portchannel1
SW3750(config-if)# switchport access vlan 201
SW3750(config-if)# channel-group 1 mode on
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/5
SW3750(config-if)# description connected to portchannel1
SW3750(config-if)# switchport access vlan 201
SW3750(config-if)# channel-group 1 mode on
SW3750(config-if)# exit
SW3750(config)# interface GigabitEthernet1/0/6
SW3750(config-if)# description connected to portchannel1
SW3750(config-if)# switchport access vlan 201
SW3750(config-if)# channel-group 1 mode on
SW3750(config-if)# exit
SW3750(config)# interface Vlan201
SW3750(config-if)# IP address 3.1.7.1 255.255.255.0
SW3750(config-if)# exit
SW3750(config)# interface Vlan202
SW3750(config-if)# IP address 3.1.8.1 255.255.255.0
SW3750(config-if)# exit
```

- Step 8** Set the load balancing algorithm to the source IP address.

```
SW3750(config)# port-channel load-balance src-ip
```



**Note** The optimal load-balance setting on the switch for traffic between the Content Acquirer and the edge Service Engine is dst-port, which is not available on the 3750, but is available on the Catalyst 6000 series.

## Switch Port-Channel Configuration for Content Acquirer and Edge Service Engine

The Cisco Catalyst 6500 Series Switch supports more port-channel load-balance options than the Cisco Catalyst 3750 Series Switch. The Cisco Catalyst 6500 Series Switch allows for full utilization of all eight port-channels grouped together between the Content Acquirer and the edge SE when dst-port is selected as the port-channel load-balance option. When the Cisco Catalyst 3750 Series Switch is used, the content is fetched by way of a single gigabit Ethernet interface because there is no dst-port load-balance option.

The following configuration recommendation for the switch port-channel load-balance option, and Content Acquirer and edge SE load-balance options, fully use all eight ports when the edge SE is fetching content from the Content Acquirer because of cache-miss requests:

- Content Acquirer port-channel load-balance option is set to **round-robin**
- Edge SE port-channel load-balance option is set to **dst-ip**
- Cisco Catalyst 6500 Series Switch instead of Cisco Catalyst 3750 Series Switch to use the dst-port option
- Cisco Catalyst 6500 Series Switch port-channel load-balance option is set to **dst-port**

## Verifying Port Channel Configuration

To verify the setup before application traffic is sent, use the following commands:

```
SE# clear statistics all
SE# show interface portChannel 1
Interface PortChannel 1 (2 physical interface(s)):
GigabitEthernet 3/0 (active)
GigabitEthernet 4/0 (active)
GigabitEthernet 5/0 (active)
GigabitEthernet 6/0 (active)
-----
Type:Ethernet
Ethernet address:00:04:23:D8:86:02
Internet address:3.1.7.73
Broadcast address:3.1.7.255
Netmask:255.255.255.0
Maximum Transfer Unit Size:1500
Metric:1
Packets Received: 28
Input Errors: 0
Input Packets Dropped: 0
Input Packets Overruns: 0
Input Packets Frames: 0
Packet Sent: 40
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length:0
Collisions: 0
Flags:UP BROADCAST RUNNING MASTER MULTICAST

SE# show interface portChannel 2
Interface PortChannel 2 (4 physical interface(s)):
GigabitEthernet 1/0 (active)
GigabitEthernet 2/0 (active)
-----
Type:Ethernet
Ethernet address:00:30:48:33:01:26
Internet address:3.1.8.200
```

## Configuring Port Channel

```

Broadcast address:3.1.8.255
Netmask:255.255.255.0
Maximum Transfer Unit Size:1500
Metric:1
Packets Received: 6
Input Errors: 0
Input Packets Dropped: 0
Input Packets Overruns: 0
Input Packets Frames: 0
Packet Sent: 0
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length:0
Collisions: 0
Flags:UP BROADCAST RUNNING MASTER MULTICAST

```

To verify the setup after application traffic is sent, use the following:

```

SE# show interface portChannel 1
Interface PortChannel 1 (4 physical interface(s)):
GigabitEthernet 3/0 (active)
GigabitEthernet 4/0 (active)
GigabitEthernet 5/0 (active)
GigabitEthernet 6/0 (active)
-----
Type:Ethernet
Ethernet address:00:04:23:D8:86:02
Internet address:3.1.7.73
Broadcast address:3.1.7.255
Netmask:255.255.255.0
Maximum Transfer Unit Size:1500
Metric:1
Packets Received: 1875
Input Errors: 0
Input Packets Dropped: 0
Input Packets Overruns: 0
Input Packets Frames: 0
Packet Sent: 5221
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length:0
Collisions: 0
Flags:UP BROADCAST RUNNING MASTER MULTICAST

SE# show interface portChannel 2
Interface PortChannel 2 (2 physical interface(s)):
GigabitEthernet 1/0 (active)
GigabitEthernet 2/0 (active)
-----
Type:Ethernet
Ethernet address:00:30:48:33:01:26
Internet address:3.1.8.200
Broadcast address:3.1.8.255
Netmask:255.255.255.0
Maximum Transfer Unit Size:1500
Metric:1
Packets Received: 21
Input Errors: 0
Input Packets Dropped: 0
Input Packets Overruns: 0

```

```

Input Packets Frames: 0
Packet Sent: 0
Output Errors: 0
Output Packets Dropped: 0
Output Packets Overruns: 0
Output Packets Carrier: 0
Output Queue Length:0
Collisions: 0
Flags:UP BROADCAST RUNNING MASTER MULTICAST

```

In the Devices Table page on the CDSM (**Devices > Devices**), the SE or SR status should be “Online.” The IP address for the device always shows the IP address of the port channel’s primary interface.

## Configuring Last-Resort Routing

Last-resort routing is applicable when load-based routing is enabled and all Service Engines have exceeded their thresholds, all Service Engines in the domain are offline, or no Service Engines have been assigned to the domain. The Service Router can redirect requests to a configurable alternate domain when all Service Engines serving a client network region are overloaded.



**Note** If the last-resort domain is not configured and the Service Engine thresholds are exceeded, requests are redirected to the Origin server. To disable Origin server redirect, see the “[Content Origins](#)” section on [page 5-1](#).

To configure last-resort routing, use the **service-router lastresort domain domain alternate alternate** global configuration command, where *domain* is the service routing domain name, and *alternate* is where to route requests.

```
service-router lastresort domain domain alternate alternate
```

In the example below, srfqdn.cisco.com is the service routing domain name, and www.cisco.com is the alternate domain name.

```

SR(config)# service-router ?
      lastresort Configure lastresort domain
      leastloaded Enable Load Based Routing
      location-based-routing Configure location based routing
SR(config)# service-router lastresort ?
      domain Configure domain
SR(config)# service-router lastresort domain srfqdn.cisco.com ?
      alternate Configure alternate domain
SR(config)# service-router lastresort domain srfqdn.cisco.com alternate ?
      WORD Configure alternate domain name
SR(config)# service-router lastresort domain srfqdn.cisco.com alternate www.cisco.com ?
      <cr>
SE(config)# service-router lastresort domain srfqdn.cisco.com alternate www.cisco.com

```

For information on configuring an error domain in which to redirect clients to that are not part of the coverage zone or configuring the translator URL option, see the “[Configuring Last-Resort Routing](#)” section on [page 4-124](#) or see the **service-router** command in *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference*.

You can also configured a port number for the alternate domain, error domain, and URL translator. The default port number is 80. For more information see the “[Configuring Last-Resort Routing](#)” section on [page 4-124](#) or see the **service-router** command in *Cisco Videoscape Distribution Suite, Internet Streamer 4.0 Command Reference*.

# Configuring Standby Interfaces

You can configure one or more interfaces to act as a backup interface (a standby interface) for another interface on a Service Engine. This feature is called *standby interface support*. Standby groups, which are logical groups of interfaces, are used to implement this feature. When an active network interface fails (because of cable trouble, Layer 2 switch failure, high error count, or other failures) and that interface is part of a standby group, a standby interface can become active and take the load off the failed interface.

A standby group must have at least two interfaces. Interfaces that are part of a standby group are called member interfaces. After you create a standby group, you define which interfaces should be assigned to this logical group. As part of defining the member interfaces, you specify the priority of each member interface in a standby group. The member interface with the highest assigned priority is the active interface for that particular standby group. If the active interface fails, the operational member interface with the next highest priority in the standby group comes up, and so forth. If all member interfaces of a particular standby group are down and then one of the member interfaces comes up, the VDS-IS software detects this situation and brings up the standby group on the member interface that just came up.

The failure or failover of member interfaces within a standby group triggers alarms and traps (if alarms and traps are enabled on the Service Engine). Alarms are sent out when failover occurs between member interfaces in a standby group. Specifically, minor alarms are sent out when member interfaces fail, and these alarms are cleared automatically when the interface failover has been successfully completed. Major alarms are sent out if the standby group goes down (no member interface in a standby group can be brought up).


**Note**

A physical interface can belong to more than one standby group, and a single interface can act as a standby interface for more than one standby group.

To configure standby interfaces, interfaces are logically assigned to standby groups. The following rules define the standby group relationships:

- Each standby group is assigned a unique standby IP address, shared by all member interfaces of the standby group. The IP address of the standby group is shared among the member interfaces; however, only the active interface of the standby group uses this shared IP address at any one time. This shared IP address is configured as an alias on the active interface.
- Duplex and speed settings of the member interfaces can be configured for better reliability.
- If a physical interface is a member of a port-channel group, it cannot join a standby group. If a physical interface is a member of a standby group, it cannot join a port-channel group.
- Maximum number of standby groups on a Service Engine is four.


**Note**

Interface IP addresses and standby group IP addresses must be on different subnets to ensure reliable operation. You can use dummy IP addresses in the private address space to serve as interface primary IP addresses, and use the real Service Engine IP address to serve as the standby group IP address in a different subnet to satisfy this requirement. When dummy IP addresses are used, these interface IP addresses serve only as substitutes to bring up the interface. For example, the Service Engine interface requires an IP address on an interface for initialization. Make sure to configure the interface default gateway using the **ip default-gateway** global configuration command instead of the **ip route** command.

- Each interface in a standby group is assigned a priority. The operational interface with the highest priority in a standby group is the active interface. Only the active interface uses the group IP address.

- Priority of an interface in a standby group can be changed at run time. The member interface that has the highest priority after this change becomes the new active interface (the default action is to preempt the currently active interface if an interface with higher priority exists).
- Maximum number of errors allowed on the active interface before the interface is shut down and the standby is brought up is configured with the **errors** option, which is disabled by default.

**Tip**

If an interface belongs to more than one standby group, you can configure the interface with a different priority in each standby group for better load balancing. For example, interfaces gigabit Ethernet 0/0 and gigabit Ethernet 0/1 are both in Standby Group 1 and in Standby Group 2. If you configure gigabit Ethernet 0/0 with the highest priority in Standby Group 1 and configure gigabit Ethernet 0/1 with the highest priority in Standby Group 2, Standby Group 1 uses gigabit Ethernet 0/0 as the active interface, while Standby Group 2 uses gigabit Ethernet 0/1 as the active interface. This configuration allows each interface to back up the other one, if one of them fails.

Use the **interface standby** global configuration command to create standby groups on Service Engines.

**Note**

Unlike port channels, standby groups do not support IP ACLs at a group level. However, you can configure a member interface of a standby group to support an IP ACL at the interface level. For example, you can individually configure the two member interfaces of Standby Group 1 (the gigabit Ethernet 0/0 interface and the gigabit Ethernet 0/1 interface) to support an IP ACL named ACL1 but you cannot configure the Standby Group 1 to support ACL1.

To configure an interface to be a backup for another interface, use the **standby** interface configuration command. To restore the default configuration of the interface, use the **no** form of this command.

```
standby group_number {description text | errors max-errors | ip ip-address netmask | priority priority_level | shutdown}
no standby group_number {description text | errors max-errors | ip ip-address netmask | priority priority_level | shutdown}
```

**Syntax Description**

<b>group_number</b>	Standby group number (1–4).
<b>description</b>	(Optional) Sets the description for the specified interface.
<b>text</b>	Description for the specified interface. The maximum length of the description text is 240 characters.
<b>errors</b>	Sets the maximum number of errors allowed on the active interface before the interface is shut down and the standby interface is brought up. This option is disabled by default.
<b>max-errors</b>	Maximum number of errors (1–2147483647).
<b>ip</b>	Sets the IP address for the specified standby group (Standby Group 1, 2, 3, or 4).
<b>ip-address</b>	IP address of the specified standby group (Standby Group 1, 2, 3, or 4). The group IP address and netmask of a standby group must be configured on all the member interfaces.
<b>netmask</b>	Netmask of the specified standby group (Standby Group 1, 2, 3, or 4).

## Configuring Standby Interfaces

---

<b>priority</b>	Sets the priority of the member interface within a standby group. The priority of a member interface can be changed at run time. The member interface that has the highest priority after this change becomes the new active interface (the default action is to preempt the currently active interface if an interface with higher priority exists).
<i>priority_level</i>	Each member interface is assigned a priority number. The member interface with the highest priority number is the active interface for that standby group. Only the active interface uses the group IP address.  If the <b>priority</b> option is specified without a priority number, the default value of 100 is used.
<b>shutdown</b>	(Optional) Shuts down the specified standby group (Standby Group 1, 2, 3, or 4). You can shut down a standby group even if you have not configured a group IP address of the standby group.  <b>Note</b> When a standby group is shut down, all the alarms previously raised by this standby group are cleared.

---

## Examples

The following example configures three gigabit Ethernet interfaces to be part of the same standby group, with interface 1/0 as the active interface:

```
Console(config-if)# interface GigabitEthernet 1/0 standby 2 priority 300
Console(config-if)# interface GigabitEthernet 2/0 standby 2 priority 200
Console(config-if)# interface GigabitEthernet 3/0 standby 2 priority 100
Console(config-if)# interface standby 2 errors 1000
```

The following example displays information about the standby group configuration by entering the **show standby** EXEC command. In the following sample command output, one standby group (Standby Group 1) is configured on this Service Engine. The command output also shows which member interface is the active interface. In this case, the active interface is the gigabit Ethernet slot 3/port 0 interface.

```
ServiceEngine# show standby
Standby Group:1
IP address: 172.16.10.10, netmask: 255.255.254.0
Maximum errors allowed on the active interface: 10000
    Member interfaces:
        GigabitEthernet 3/0 priority: 300
        GigabitEthernet 3/1 priority: 200
        GigabitEthernet 3/2 priority: 100

    Active interface: GigabitEthernet 3/0
```



**Note** To display information about a specific standby group configuration, enter the **show interface standby group\_number** EXEC command.

The following example creates a standby group, Standby Group 1:

```
ServiceEngine# configure
ServiceEngine(config)# interface standby 1
ServiceEngine(config-if)#
```

The following example assigns a group IP address of 10.10.10.10 and a netmask of 255.0.0.0 to Standby Group 1:

```
ServiceEngine(config-if)# IP address 10.10.10.10 255.0.0.0
ServiceEngine(config-if)# errors 500
```

The following example shows how to add two gigabit Ethernet interfaces to Standby Group 1 and then assign each of these member interfaces a priority within the group:

1. Add a gigabit Ethernet interface 0/0 to Standby Group 1 and assign a priority of 150.

```
ServiceEngine(config)# interface GigabitEthernet 0/0
ServiceEngine(config-if)# standby 1 priority 150
```

2. Add a second gigabit Ethernet interface 0/1 to Standby Group 1 with the default priority value of 100.

```
ServiceEngine(config)# interface GigabitEthernet 0/1
ServiceEngine(config-if)# standby 1
ServiceEngine(config-if)# exit
ServiceEngine(config)#
```

Because gigabit Ethernet 0/0 is assigned the highest priority (a priority number of 150) of all the member interfaces in the group, it is chosen as the active interface for the group if it can be brought up.

The following example removes the gigabit Ethernet 0/1 interface from Standby Group 1 using the **no** form of the **standby** command:

```
ServiceEngine(config)# interface FastEthernet 0/1
ServiceEngine(config-if)# no standby 1
ServiceEngine(config-if)# exit
ServiceEngine(config)#
```

The following example shows how to shut down Standby Group 1. When a standby group is shut down, all the alarms previously raised by this standby group are cleared.

```
ServiceEngine(config)# interface standby 1
ServiceEngine(config-if)# shutdown
ServiceEngine(config)# exit
```

The following example shows how to tear down Standby Group 1:

```
ServiceEngine(config)# interface standby 1
ServiceEngine(config-if)# no IP address 10.10.10.10 255.0.0.0
Please remove member interface(s) from this standby group first.
ServiceEngine(config)# interface GigabitEthernet 2/0
ServiceEngine(config-if)# no standby 1
ServiceEngine(config-if)# exit
ServiceEngine(config)# interface standby 1
ServiceEngine(config-if)# no IP address 10.10.10.10 255.0.0.0
ServiceEngine(config-if)# exit
ServiceEngine(config)# no interface standby 1
ServiceEngine(config)# exit
```

## Standby Interface with Switch Failover Configuration Procedure

This procedure describes how to configure a standby interface for two port channels and a standby interface for two management interfaces on a device with a total of six interfaces.

To configure a standby interface with two port channels, follow these steps:

- 
- Step 1** Configure gigabit Ethernet 1/0 and gigabit Ethernet 2/0 as management interfaces and create one standby interface for redundancy.

```
SE(config)# interface GigabitEthernet 1/0
SE(config-if)# standby 2 priority 200
```

## Configuring Standby Interfaces

```
SE(config-if)# exit
SE(config)# interface GigabitEthernet 2/0
SE(config-if)# standby 2
SE(config-if)# exit
SE(config-if)# interface Standby 2
SE(config-if)# description for management
SE(config-if)# IP address 4.0.7.127 255.255.255.0
SE(config-if)# exit
```

- Step 2** Add gigabit Ethernet 3/0 and gigabit Ethernet 4/0 to port channel 1, add gigabit Ethernet 5/0 and gigabit Ethernet 6/0 to port channel 2, and create a standby interface for these two port channels for redundancy.

```
SE(config)# interface GigabitEthernet 3/0
SE(config-if)# channel-group 1
SE(config-if)# exit
SE(config)# interface GigabitEthernet 4/0
SE(config-if)# channel-group 1
SE(config-if)# exit
SE(config)# interface GigabitEthernet 5/0
SE(config-if)# channel-group 2
SE(config-if)# exit
SE(config)# interface GigabitEthernet 6/0
SE(config-if)# channel-group 2
SE(config-if)# exit
SE(config)# interface PortChannel 1
SE(config-if)# standby 1 priority 120
SE(config-if)# exit
SE(config)# interface PortChannel 2
SE(config-if)# standby 1 priority 200
SE(config-if)# exit
SE(config)# interface Standby 1
SE(config-if)# description for traffic
SE(config-if)# IP address 7.35.0.7 255.255.0.0
SE(config-if)# exit
SE(config)# primary-interface Standby 1
```



**Note** Port channel 1 is bundled to switch 1 and port channel 2 is bundled to switch 2.



## Verifying the Videoscape Distribution Suite, Internet Streamer

---

This appendix covers the steps to test the Videoscape Distribution Suite, Internet Streamer (VDS-IS) by using the different media players.

- [Verifying the Web Engine, page J-1](#)
- [Verifying the Windows Media Streaming Engine, page J-9](#)
- [Verifying the Movie Streamer Engine, page J-13](#)
- [Verifying the Flash Media Streaming Engine, page J-21](#)

The VDS-IS network topology example used in these procedures consists of the following devices:

- 2 CDE220s configured as Service Engines (SEs)
  - NE-DEMO-SE1 — Tier 1 location
  - NE-DEMO-SE2 — Tier 2 location
- 1 CDE205 configured as a Service Router (SR)
  - NE-DEMO-SR — Tier 2 location
- 1 CDE205 configured as a Content Delivery System Manager (CDSM)
  - NE-DEMO-CDSM

## Verifying the Web Engine

This section consists of the following procedures:

- [Verifying Preingested Web Content](#)
- [Verifying Dynamically Ingested Web Content](#)

## Verifying Preingested Web Content



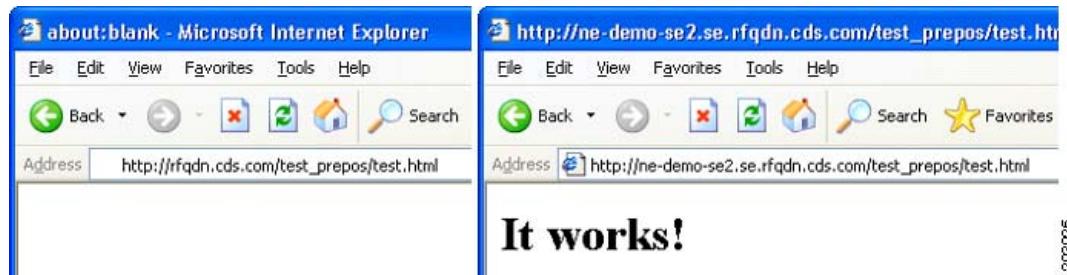
**Note**

Content must be preingested. See the “Configuring Delivery Services” section on page 5-1 for more information. Verify that the content has been pre-positioned by using the **show distribution object-status name-of-object** command.

## Verifying the Web Engine

- 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](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 J-1](#) shows the initial URL on the left and the redirection on the right.

**Figure J-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 web-engine** command. In this case, the Service Router redirected the request to NE-DEMO-SE2, which served the request.

```
NE-DEMO-SE1# show statistics web-engine
```

```
HTTP Request Info Statistics
-----
Num Lookups          : 0
Preposition Hit     : 0
External Hit         : 0
Cache Hit            : 0
Cache Miss           : 0
Partial Cache Hit   : 0
Cache Bypass         : 0
Live Miss            : 0
Live Hit             : 0
ASX Meta Response   : 0

HTTP Request Type Statistics
-----
Get Requests          : 0
Post Requests         : 0
Head Requests         : 0
Range Requests Received : 0
Range Requests Sent   : 0
Revalidation Requests Received : 0
Revalidation Requests Sent : 0
Liveness Query        : 0
WMT(http) Redirected Requests : 0
Local Requests         : 0
Play Live Requests    : 0
Total Outgoing Requests : 0

HTTP Authorization Statistics
-----
Authorization Allow   : 0
Authorization No Cache: 0
Authorization Force Revalidate : 0
Authorization Deny    : 0
Authorization Rewrite : 0
Authorization GenerateSign : 0
```

```

Authorization Redirect      :          0
Authorization Resolve     :          0

WMT(http) Rule Statistics
-----
Allow                      :          0
Block                     :          0
Url Redirect               :          0
Url Rewrite                :          0
Validate Url Signature    :          0
No Cache                  :          0

HTTP Error Statistics
-----
Client Errors              :          0
Server Errors              :          0
Bad Requests               :          0
Error Response Miss       :          0
Error Response Hit        :          0

Statistics was last cleared on Thursday, 09-Sep-2010 14:15:52 PDT.

NE-DEMO-SE2# show statistics web-engine

HTTP Request Info Statistics
-----
Num Lookups                :          1
Preposition Hit            :          1
External Hit                :          0
Cache Hit                  :          0
Cache Miss                 :          0
Partial Cache Hit          :          0
Cache Bypass                :          0
Live Miss                  :          0
Live Hit                   :          0
ASX Meta Response          :          0

HTTP Request Type Statistics
-----
Get Requests                :          1
Post Requests               :          0
Head Requests               :          0
Range Requests Received   :          0
Range Requests Sent         :          0
Revalidation Requests Received :          0
Revalidation Requests Sent  :          0
Liveness Query              :          0
WMT(http) Redirected Requests :          0
Local Requests               :          0
Play Live Requests          :          0
Total Outgoing Requests    :          0

HTTP Authorization Statistics
-----
Authorization Allow          :          1
Authorization No Cache      :          0
Authorization Force Revalidate :          0
Authorization Deny           :          0
Authorization Rewrite        :          0
Authorization Resolve        :          0

WMT(http) Rule Statistics
-----
Allow                      :          1

```

## Verifying the Web Engine

```

Block : 0
Url Redirect : 0
Url Rewrite : 0
Validate Url Signature : 0
No Cache : 0

WMT(http) Rule Statistics
-----
Allow : 0
Block : 0
Url Redirect : 0
Url Rewrite : 0
Validate Url Signature : 0
No Cache : 0

HTTP Error Statistics
-----
Client Errors : 0
Server Errors : 0
Bad Requests : 0

Statistics was last cleared on Thursday, 09-Sep-2010 14:15:52 PDT.

```

## 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 J-2](#) shows the initial URL on the left and the redirection on the right.

**Figure J-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 J-2](#)), having cached the content as well.

- Step 2** View the HTTP request statistics by entering the **show statistics web-engine** command.

```

NE-DEMO-SE1# show statistics web-engine

HTTP Request Info Statistics
-----
Num Lookups : 1

```

Preposition Hit	:	0
External Hit	:	0
Cache Hit	:	0
Cache Miss	:	1
Partial Cache Hit	:	0
Cache Bypass	:	0
Live Miss	:	0
Live Hit	:	0
ASX Meta Response	:	0

#### HTTP Request Type Statistics

<hr/>		
Get Requests	:	1
Post Requests	:	0
Head Requests	:	0
Range Requests Received	:	0
Range Requests Sent	:	0
Revalidation Requests Received	:	0
Revalidation Requests Sent	:	0
Liveness Query	:	1
WMT(http) Redirected Requests	:	0
Local Requests	:	0
Play Live Requests	:	0
Total Outgoing Requests	:	0

#### HTTP Authorization Statistics

<hr/>		
Authorization Allow	:	1
Authorization No Cache	:	0
Authorization Force Revalidate	:	0
Authorization Deny	:	0
Authorization Rewrite	:	0
Authorization Resolve	:	0

#### WMT(http) Rule Statistics

<hr/>		
Allow	:	1
Block	:	0
Url Redirect	:	0
Url Rewrite	:	0
Validate Url Signature	:	0
No Cache	:	0

#### HTTP Error Statistics

<hr/>		
Client Errors	:	0
Server Errors	:	0
Bad Requests	:	0

Statistics was last cleared on Thursday, 09-Sep-2010 16:15:52 PDT.

```
NE-DEMO-SE2# show statistics web-engine
```

#### HTTP Request Info Statistics

<hr/>		
Num Lookups	:	1
Preposition Hit	:	0
External Hit	:	0
Cache Hit	:	0
Cache Miss	:	1
Partial Cache Hit	:	0
Cache Bypass	:	0
Live Miss	:	0
Live Hit	:	0

## Verifying the Web Engine

```

ASX Meta Response      :          0
HTTP Request Type Statistics
-----
Get Requests           :          1
Post Requests          :          0
Head Requests          :          0
Range Requests Received :          0
Range Requests Sent    :          0
Revalidation Requests Received : 0
Revalidation Requests Sent : 0
Liveness Query         :          0
WMT(http) Redirected Requests : 0
Local Requests          :          0
Play Live Requests     :          0
Total Outgoing Requests :          0

HTTP Authorization Statistics
-----
Authorization Allow     :          1
Authorization No Cache  :          0
Authorization Force Revalidate : 0
Authorization Deny       :          0
Authorization Rewrite    :          0
Authorization Resolve    :          0

WMT(http) Rule Statistics
-----
Allow                  :          1
Block                  :          0
Url Redirect           :          0
Url Rewrite            :          0
Validate Url Signature :          0
No Cache               :          0

HTTP Error Statistics
-----
Client Errors          :          0
Server Errors          :          0
Bad Requests           :          0

```

Statistics was last cleared on Thursday, 09-Sep-2010 16:17:52 PDT.

- 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 20000000
Number of cal cached assets: 1
Eviction protection is disabled.
Cache eviction-preferred-size configured is large
-----
Size   URL
-----
44    http://ofqdn.cds.com/test_cache/test.html

```

```

NE-DEMO-SE2#show cache content
Max-cached-entries is set as 20000000
Number of cal cached assets: 1
Eviction protection is disabled.
Cache eviction-preferred-size configured is large
-----
Size   URL
-----

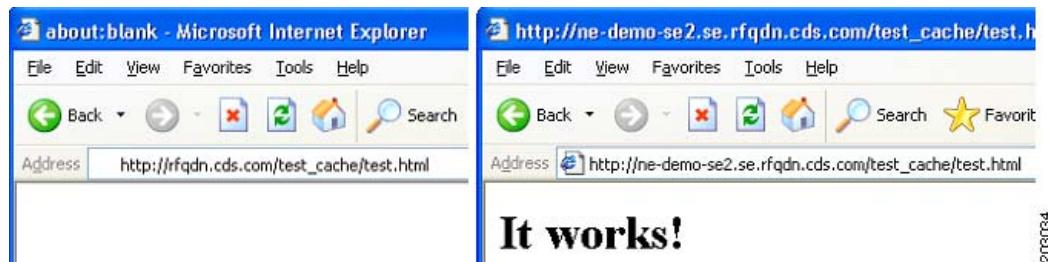
```

44 http://ofcdn.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://rfcdn.cds.com/test\\_cache/test.html](http://rfcdn.cds.com/test_cache/test.html)). **Figure J-3** shows the initial URL request on the left and the new URL on the right.

**Figure J-3 Show Statistic Requests on NE-DEMO-SE1—Cached Content**



**Step 6** View the HTTP request statistics again by entering the **show statistics web-engine** command.

```
NE-DEMO-SE1# show statistics web-engine
```

#### HTTP Request Info Statistics

	:	
Num Lookups	:	1
Preposition Hit	:	0
External Hit	:	0
Cache Hit	:	0
Cache Miss	:	1
Partial Cache Hit	:	0
Cache Bypass	:	0
Live Miss	:	0
Live Hit	:	0
ASX Meta Response	:	0

#### HTTP Request Type Statistics

	:	
Get Requests	:	1
Post Requests	:	0
Head Requests	:	0
Range Requests Received	:	0
Range Requests Sent	:	0
Revalidation Requests Received	:	0
Revalidation Requests Sent	:	0
Liveness Query	:	1
WMT(http) Redirected Requests	:	0
Local Requests	:	0
Play Live Requests	:	0
Total Outgoing Requests	:	0

#### HTTP Authorization Statistics

	:	
Authorization Allow	:	1
Authorization No Cache	:	0
Authorization Force Revalidate	:	0
Authorization Deny	:	0
Authorization Rewrite	:	0
Authorization Resolve	:	0

#### HTTP Error Statistics

## Verifying the Web Engine

```
-----
Client Errors      :          0
Server Errors     :          0
Bad Requests       :          0

Statistics was last cleared on Thursday, 09-Sep-2010 16:15:52 PDT.

NE-DEMO-SE2# show statistics web-engine

HTTP Request Info Statistics
-----
Num Lookups        :          2
Preposition Hit    :          0
External 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

HTTP Request Type Statistics
-----
Get Requests        :          2
Post Requests       :          0
Head Requests       :          0
Range Requests Received :          0
Range Requests Sent  :          0
Revalidation Requests Received : 0
Revalidation Requests Sent   : 0
Liveness Query      :          0
WMT(http) Redirected Requests : 0
Local Requests      :          0
Play Live Requests  :          0
Total Outgoing Requests :          0

HTTP Authorization Statistics
-----
Authorization Allow  :          2
Authorization No Cache :          0
Authorization Force Revalidate : 0
Authorization Deny    :          0
Authorization Rewrite :          0
Authorization Resolve :          0

HTTP Error Statistics
-----
Client Errors      :          0
Server Errors     :          0
Bad Requests       :          0

HStatistics was last cleared on Thursday, 09-Sep-2010 16:15:52 PDT.
```

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

This section consists of the following procedures:

- [Verifying Preingested Windows Media Content](#)
- [Verifying Dynamically Ingested Windows Media Content](#)
- [Verifying Windows Media Live Content Playback](#)

## Verifying Preingested Windows Media Content


**Note**

Content must be preingested. See the “Configuring Delivery Services” section on page 5-1 for more information. Verify that the content has been pre-positioned by using the **show distribution object-status name-of-object** command.

**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 J-4) and click **OK**. In the example, this is “rtsp://rfqdn.cds.com/test\_prepos/test.wmv.”

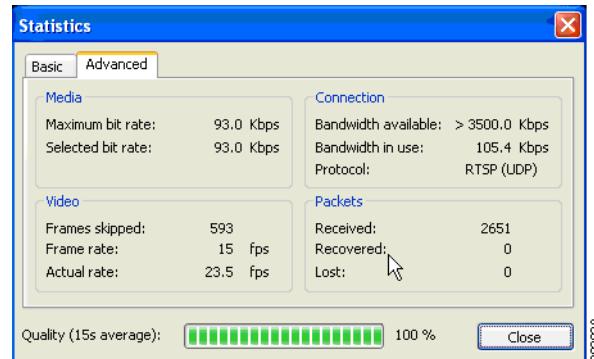
**Figure J-4**      *Open URL Dialog Box*



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 J-5).

**Figure J-5**      *Windows Media Player Statistics*



## Verifying the Windows Media Streaming Engine

- 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:
=====
Stream-Id Client-IP Type Transport Source State Pkts-sent Bytes-sent Duration BW Instance

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:
=====
Stream-Id Client-IP Type Transport Source State Pkts-sent Bytes-sent Duration BW
Instance
8895 171.70.222.171 VOD NONE LOCAL Setup 0 0 0 0
test_prepos/test.wmv
```

---

## Verifying Dynamically Ingested Windows Media Content

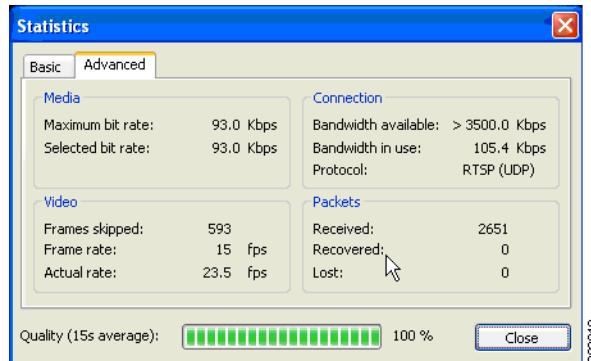
- Step 1** On the client PC, start the Windows Media Player program.
- Step 2** Choose **File > Open URL**.
- Step 3** Enter the URL of content that has not been preingested in the Open URL dialog box ([Figure J-6](#)) and click **OK**. In the example, this is “rtsp://rfqdn.cds.com/test\_cache/test.wmv.”

**Figure J-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 J-7](#)).

**Figure J-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 served 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
20548 VOD RMT_HTTP Play 6113001 21 1012 3.1.13.6
rtsp://ofqdn.cds.com/test_cache/test.wmv

Outgoing Streams:
=====
Stream-Id Client-IP Type Transport Source State Pkts-sent Bytes-sent Duration
BW Instance
27521 3.1.4.14 VOD RTSPT RMT_HTTP Play 388 3104000 19
549 test_cache/test.wmv

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:
=====
Stream-Id Client-IP Type Transport Source State Pkts-sent Bytes-sent Duration
BW Instance
12043 171.70.222.171 VOD RTSPT RMT_RTSP Play 279 2232000 13
7201 test_cache/test.wmv
```

## Verifying Windows Media Live Content Playback



- Note** Each live program uses a live Delivery Service to deliver the live program. See the “[Configuring Programs](#),” page 5-47 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 J-8](#)) and click **OK**. In the example, this is “rtsp://rfqdn.cds.com/wmtlive.”

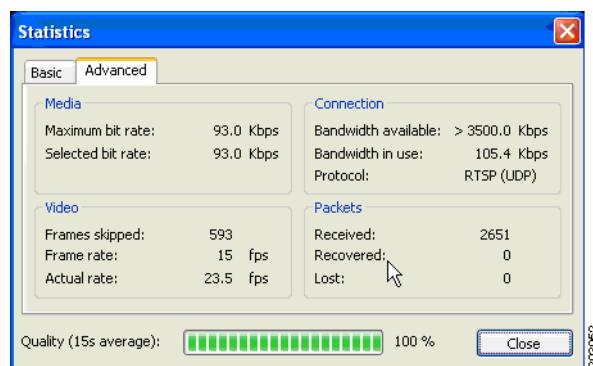
**Figure J-8** Open URL Dialog Box



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 J-9](#)).

**Figure J-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:
=====
Stream-Id Client-IP      Type Transport Source   State    Pkts-sent
Bytes-sent Duration  BW  Instance
18889      3.1.4.14     LIVE  RTSPT    RMT_HTTP Play      5393      7787492    233
288       8080

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:
=====
Stream-Id Client-IP      Type Transport Source   State    Pkts-sent Bytes-sent Duration
BW  Instance
28755      171.70.222.171 LIVE  RTSPU    RMT_RTSP Play      5582      8060408    241
288       wmtlive

```

---

## Verifying the Movie Streamer Engine

This section includes the following procedures:

- [Preparing Movie Streamer Content for Ingest](#)
- [Verifying Preingested Movie Streamer Content](#)
- [Verifying Dynamically Ingested Movie Streamer Content](#)
- [Verifying Movie Streamer Live Content Playback](#)

## 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.

---

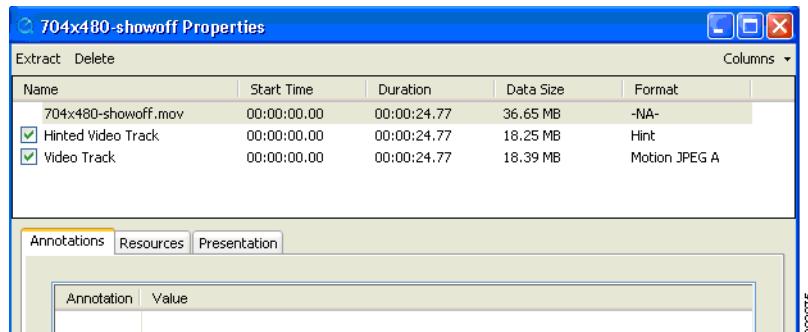
**Step 1** Launch Apple QuickTime Pro.

**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 J-10](#), then open the next movie file.

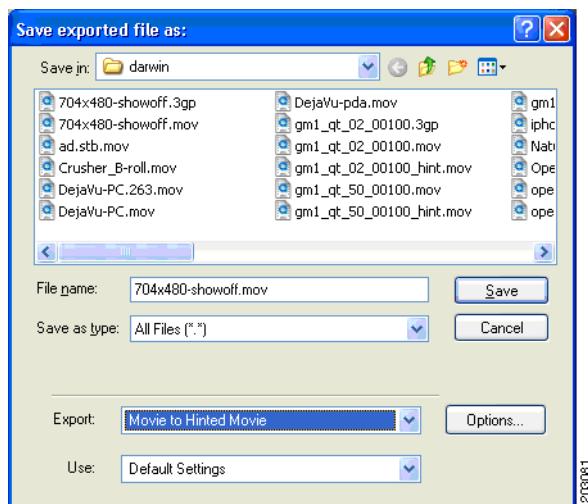
## Verifying the Movie Streamer Engine

**Figure J-10** Movie Properties Dialog Box



**Step 4** Choose **File > Export**. The Save Exported File dialog box is displayed (Figure J-11).

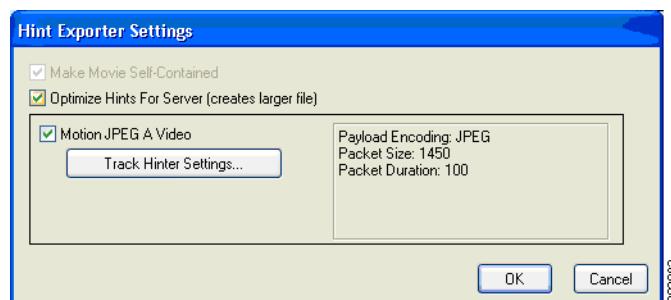
**Figure J-11** Save Exported File Dialog Box



**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 J-12).

**Figure J-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



**Note**

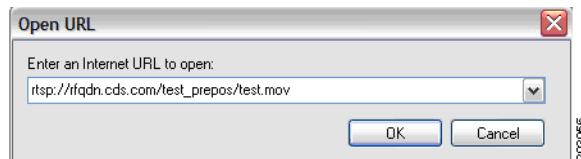
Content must be preingested. See the “Configuring Delivery Services” section on page 5-1 for more information. Verify that the content has been pre-positioned by using the **show distribution object-status name-of-object** command.

**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 J-13) and click **OK**. In the example, this URL is “rtsp://rfqdn.cds.com/test\_prepes/test.mov.”

**Figure J-13** Open URL Dialog Box

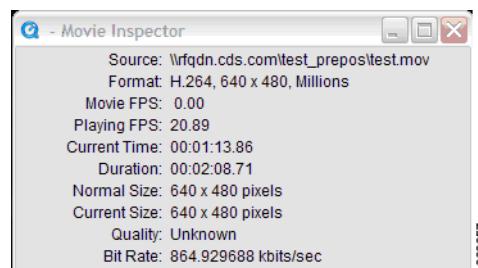


The video begins to play.

**Step 4** To view the statistics on the video file, choose **Windows > Show Movie Inspector** (Figure J-14).

The current statistics are displayed and updated as the video streams and plays.

**Figure J-14** QuickTime Player Statistics



**Step 5** To view the request flow, use the **show statistics movie-streamer all** command.

```
NE_DEMO-SE2# show statistics movie-streamer all
Movie Streamer Request Statistics
      Total
-----
Current RTSP sessions:          0
Total RTSP sessions:            1
Current RTP connections:        0
Total RTP connections:          1
```

## Verifying the Movie Streamer Engine

```

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
Total
-----
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-2007 23:53:59 UTC.

```



**Note** In this example, current connections and bandwidth are all zero because the movie has finished playing at the time the statistics were displayed.



**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.

**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.

```

NE_DEMO-SE2# show statistics movie-streamer all
Movie Streamer Request Statistics
Total
-----
Current RTSP sessions: 1
Total RTSP sessions: 2
Current RIP 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
Total
-----
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

...Omitted contents

Overall Traffic
-----
Incoming Bytes: 0 Bytes

```

## Verifying the Movie Streamer Engine

```
Outgoing Bytes: 14490660 Bytes
Total Bytes: 14490660 Bytes
```

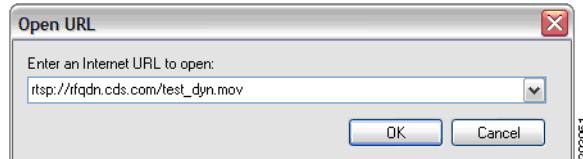
...Omitted contents

## Verifying Dynamically Ingested Movie Streamer Content

When content requested by a client is not in the VDS-IS, 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 VDS-IS in the Open URL dialog box (Figure J-15) and click **OK**. In the example, this is “rtsp://rfqdn.cds.com/test\_dyn.mov.”

**Figure J-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
Total
-----
Current RTSP sessions: 1
Total RTSP sessions: 4
Current RIP connections: 1
Total RTP connections: 4

...Omitted contents

Movie Streamer Bandwidth Usage Statistics
Total
-----
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
```

...Omitted contents

Overall Traffic

-----

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
Total RTSP sessions: 0
Current RIP 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

...Omitted contents

Overall Traffic
-----
Incoming Bytes: 13283705 Bytes
Outgoing Bytes: 0 Bytes
    Total Bytes: 13283705 Bytes

...Omitted contents

```

---

## Verifying Movie Streamer Live Content Playback



**Note** Each live program uses a live Delivery Service to deliver the live program. See the “[Configuring Programs](#),” page 5-47 for more information.

Live streaming of Movie Streamer content requires a Session Description Protocol (SDP) file. The SDP file used in this procedure is the following:

```

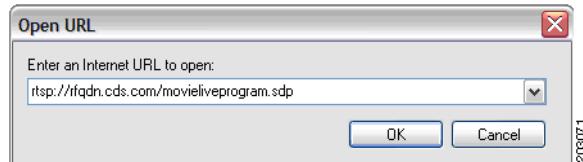
v=0
o=QTSS_Play_List 2079157989 2079176415 IN IP4 171.71.50.216
s=C:\Program Files\Darwin Streaming Server\Playlists\untitled\unti@
c=IN IP4 127.0.0.1
b=AS:94
t=0 0
a=x-broadcastcontrol:RTSP
m=video 0 RTP/AVP 96
b=AS:79
a=rtpmap:96 X-SV3V-ES/90000
a=control:trackID=1
m=audio 0 RTP/AVP 97
b=AS:14
a=rtpmap:97 X-QDM/22050/2
a=control:trackID=2
a=x-bufferdelay:4.97

```

## Verifying the Movie Streamer Engine

- 
- 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 J-16) and click **OK**. In the example, this is “rtsp://rfqdn.cds.com/movieliveprogram.sdp.”

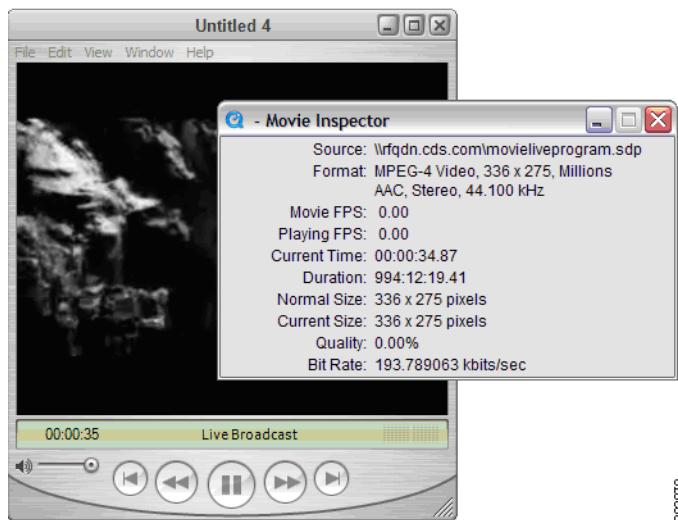
**Figure J-16** Open URL Dialog Box



The video begins to play.

- Step 4** To view the statistics on the video file, choose **Window > Show Movie Inspector** (Figure J-17). The current statistics are displayed and updated as the video streams and plays.

**Figure J-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
Total 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
...Omitted contents

Overall Traffic
-----
Incoming Bytes:        4478769 Bytes
Outgoing Bytes:        4499370 Bytes
    Total Bytes:         8978139 Bytes

...Omitted contents

NE_DEMO-SE2# show statistics movie-streamer all
Movie Streamer Request Statistics
    Total
-----
Current RTSP sessions:      0
Total RTSP sessions:        0
Current RIP connections:    0
Total RTP connections:      1

...Omitted contents

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

...Omitted contents

Overall Traffic
-----
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-2007 20:09:42 UTC.

```

---

## Verifying the Flash Media Streaming Engine

This section consists of the following procedures:

- [Verifying Flash Media Streaming Preingested Content](#)

**Verifying the Flash Media Streaming Engine**

- [Verifying Flash Media Streaming Dynamically Ingested Content](#)
- [Verifying Flash Media Streaming—Live Streaming](#)

## Verifying Flash Media Streaming Preingested Content



**Note** Content must be preingested. This was accomplished in the “[Configuring Delivery Services](#)” section on [page 5-1](#). 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/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” 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/path/foo.flv` format for VOD streams, but the SE replaces the “vod” directory with the string specified in the **flash-media-streaming application-virtual-path vod map** command.

Use the **flash-media-streaming application-virtual-path vod 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” directory to “media” for the go-tv-stream.com origin server, use the **flash-media-streaming application-virtual-path vod map media** command.

To monitor live streaming, use the **show statistics flash-media-streaming** command and the **show flash-media-streaming livestreams** command.

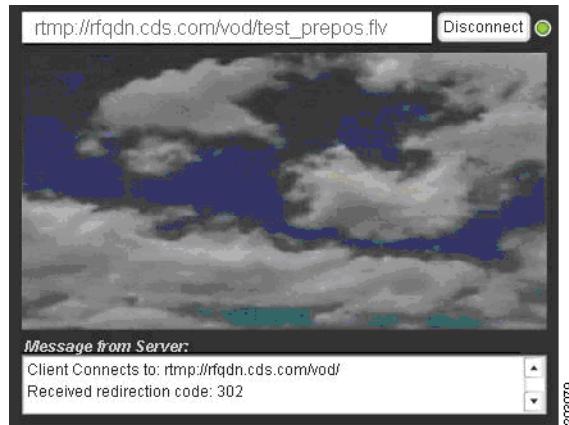
---

**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 J-18](#)) and click **Go**. In the example, this is “`rtmp://rfqdn.cds.com/vod/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 J-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-2007 37:22:58 UTC.

Connections
-----
Current Connections
Total : 1
VOD : 1
LIVE : 0
DVRCast : 0
Proxy : 0
Max Concurrent : 1
Total Connections
Total : 1
VOD : 1
LIVE : 0
DVRCast : 0
Proxy : 0

VOD Streaming
-----
Current Connections : 1
Total Connections : 1
DownStream Bytes : 880668
UpStream Bytes : 0
DownStream BW : 0 Kbps
Preposition Hit : 1
External Hit : 0
Cache Hit : 0
Cache Miss : 0
Proxy Case : 0
Cache Hit Percentage : 0.00
Local Disk Reads : 3
HTTP Based Reads : 0
Bytes From Local Disk: 880668
```

## Verifying the Flash Media Streaming Engine

```

Bytes Through HTTP   :          0
Ignore Query String :          0

Live Streaming
-----
Current Connections   :          0
Total Connections    :          0
UpStream BW           :          0 Kbps
DownStream BW          :          0 Kbps
UpStream Bytes         :          0
DownStream Bytes        :          0
Downstream CDS-IS total conn.: 0
Ignore Query String   :          0

DVRCast Streaming
-----
Current Connections   :          0
Total Connections    :          0
UpStream BW           :          0 Kbps
DownStream BW          :          0 Kbps
UpStream Bytes         :          0
DownStream Bytes        :          0
Ignore Query String   :          0

Proxy Streaming
-----
Current Connections   :          0
Total Connections    :          0
UpStream BW           :          0 Kbps
DownStream BW          :          0 Kbps
UpStream Bytes         :          0
DownStream Bytes        :          0

Rules
-----
Action Allow          :          0
Action Block          :          0
Validate url Sign     :          0
URL Signing errors:
    Invalid Client      :          0
    Invalid Signature    :          0
    No signing           :          0
    Expired URL          :          0
Auth server validation:
    Auth Server Allow    :          0
    Auth Server Deny     :          0

SWF Verification :
-----
Requests
    Performed          :          0
    Failed              :          0
    Successful          :          0
    Bypassed             :          0
    Memory Hash Hit     :          0
    Memory Hash Calculated: 0
    Local SWF Hit       :          0
    Preposition SWF     :          0
    SWF Cache Hit       :          0
    SWF Cache Miss      :          0
    SWF Proxy            :          0
Errors
    SWF Fetch Error     :          0
    Local SWF Read Error: 0

```

```

Cached SWF Read Error : 0
SWF File not found : 0
SWF Incorrect Depth : 0
SWF Hash Match Fail : 0
SWF Hash Partial : 0
Edge SWF Cache Miss : 0
SWF Response Timeout : 0
SWF Client Unsupported: 0
SWF Wrong Version : 0

Error
-----
Disk Error
    File Open Error : 0
    File Read Error : 0
    File GetAttributes Error : 0
    File Close Error : 0

HTTP Error
    Invalid Error : 0
    Server Error : 0
    Media Not Found : 0
    Media Unauthorized : 0
    Invalid Request : 0
    Bad Gateway : 0
    Service Unavailable : 0
    Gateway Timeout : 0
    Request Failed : 0
    Invalid Response : 0
    Too many Redirect : 0
    Invalid Redirect : 0
    Invalid Cache Type : 0

Server
-----
Total UpStream BW : 0 Kbps
Total DownStream BW : 0 Kbps
Total UpStream Bytes : 0
Total DownStream Bytes : 880668
Total Server Bytes : 880668

Performance
-----
Server Up Time : 816 S
Mem Usage : 5 %
Max Mem Usage : 5 %
Total Messages Dropped: 0

Num of Active VOD Instances : 1
Num of Active Live Instances : 0
Num of Active DVRCast Instances : 0

Flash Video Cache Statistics
-----
Hits : 0
Misses : 0
Released : 0
Bytes in cache : 0
Bytes in use : 0
Disk Usage : 4096

```

---

## 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 20000000
Number of cal cached assets: 0
Eviction protection is disabled.
Cache eviction-preferred-size configured is large
-----
Size          URL
-----
```

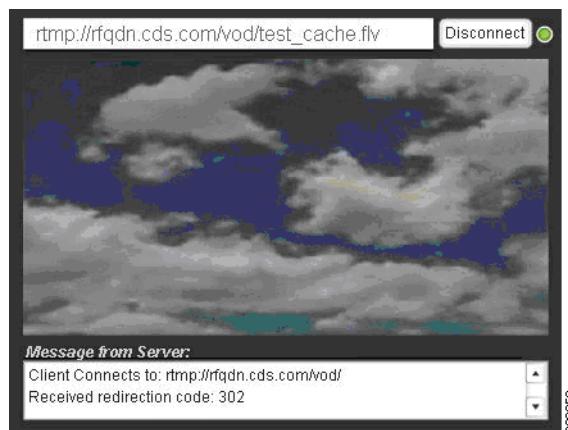
- Step 2** On the client PC, start the Adobe Flash Player.

- Step 3** Enter the URL of the flash file in the text box (Figure J-19) and click **Go**. In the example, this is “rtmp://rfqdn.cds.com/vod/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 J-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-2007 37:22:58 UTC.

Connections
-----
Current Connections
```

```

Total : 1
VOD : 1
LIVE : 0
DVRCast : 0
Proxy : 0
Max Concurrent : 1
Total Connections
Total : 1
VOD : 1
LIVE : 0
DVRCast : 0
Proxy : 0

VOD Streaming
-----
Current Connections : 1
Total Connections : 1
DownStream Bytes : 0
UpStream Bytes : 0
DownStream BW : 0 Kbps
Preposition Hit : 0
External Hit : 0
Cache Hit : 0
Cache Miss : 1
Proxy Case : 0
Cache Hit Percentage : 0.00
Local Disk Reads : 2
HTTP Based Reads : 1
Bytes From Local Disk: 587112
Bytes Through HTTP : 293556
Ignore Query String : 0

Live Streaming
-----
Current Connections : 0
Total Connections : 0
UpStream BW : 0 Kbps
DownStream BW : 0 Kbps
UpStream Bytes : 0
DownStream Bytes : 0
Downstream CDS-IS total conn.: 0
Ignore Query String : 0

DVRCast Streaming
-----
Current Connections : 0
Total Connections : 0
UpStream BW : 0 Kbps
DownStream BW : 0 Kbps
UpStream Bytes : 0
DownStream Bytes : 0
Ignore Query String : 0

Proxy Streaming
-----
Current Connections : 0
Total Connections : 0
UpStream BW : 0 Kbps
DownStream BW : 0 Kbps
UpStream Bytes : 0
DownStream Bytes : 0

Rules
-----

```

## Verifying the Flash Media Streaming Engine

```

Action Allow      :          0
Action Block     :          0
Validate url Sign :          0
URL Signing errors:
    Invalid Client   :          0
    Invalid Signature :          0
    No signing       :          0
    Expired URL     :          0
Auth server validation:
    Auth Server Allow :          0
    Auth Server Deny  :          0

SWF Verification :
-----
Requests
    Performed      :          0
    Failed          :          0
    Successful      :          0
    Bypassed         :          0
    Memory Hash Hit :          0
    Memory Hash Calculated: 0
    Local SWF Hit   :          0
    Preposition SWF :          0
    SWF Cache Hit   :          0
    SWF Cache Miss  :          0
    SWF Proxy        :          0
Errors
    SWF Fetch Error :          0
    Local SWF Read Error : 0
    Cached SWF Read Error : 0
    SWF File not found : 0
    SWF Incorrect Depth : 0
    SWF Hash Match Fail : 0
    SWF Hash Partial : 0
    Edge SWF Cache Miss : 0
    SWF Response Timeout : 0
    SWF Client Unsupported: 0
    SWF Wrong Version : 0

Error
-----
Disk Error
    File Open Error   :          0
    File Read Error   :          0
    File GetAttributes Error : 0
    File Close Error  :          0

HTTP Error
    Invalid Error     :          0
    Server Error      :          0
    Media Not Found   :          0
    Media Unauthorized: 0
    Invalid Request   :          0
    Bad Gateway       :          0
    Service Unavailable: 0
    Gateway Timeout   :          0
    Request Failed    :          0
    Invalid Response  :          0
    Too many Redirect :          0
    Invalid Redirect  :          0
    Invalid Cache Type: 0

Server
-----
```

```

Total UpStream BW      :          0 Kbps
Total DownStream BW   :          0 Kbps
Total UpStream Bytes  :          0
Total DownStream Bytes : 587112
Total Server Bytes    : 587112

Performance
-----
Server Up Time       : 933 S
Mem Usage            : 5 %
Max Mem Usage        : 5 %
Total Messages Dropped: 0

Num of Active VOD Instances : 1
Num of Active Live Instances : 0
Num of Active DVRCast Instances : 0

Flash Video Cache Statistics
-----
Hits                : 0
Misses              : 0
Released             : 0
Bytes in cache       : 0
Bytes in use          : 0
Disk Usage           : 4096

```

- 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 20000000
Number of cal cached assets: 1
Eviction protection is disabled.
Cache eviction-preferred-size configured is large
-----
Size      URL
-----
293556   http://ofcdn.cds.com/vod/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 a CDS 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>`.

## Verifying the Flash Media Streaming Engine

For example, if the URL was rtmp://Temp4.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-2007 37:22:58 UTC.

Connections
-----
Current Connections
Total : 1
VOD : 0
LIVE : 1
DVRCast : 0
Proxy : 0
Max Concurrent : 1
Total Connections
Total : 3
VOD : 0
LIVE : 1
DVRCast : 0
Proxy : 0

...Omitted contents

Live Streaming
-----
Current Connections : 1
Total Connections : 1
UpStream BW : 0 Kbps
DownStream BW : 274 Kbps
UpStream Bytes : 3194
DownStream Bytes : 124362967
Downstream CDS-IS total conn.: 1

...Omitted contents
```

- 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
-----
OsUrl : 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

...Omitted contents
```

- 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-2007 37:22:58 UTC.

        Current Connections
Total          :           1
VOD           :           0
LIVE          :           1
DVRCast       :           0
Proxy         :           0
Max Concurrent:           1

Total Connections
Total          :           1
VOD           :           0
LIVE          :           0
DVRCast       :           0
Proxy         :           0

...Omitted contents

Live Streaming
-----
UpStream BW    :           0 kbps
DownStream BW   :         274 kbps
UpStream Bytes  :         3487
DownStream Bytes : 149456451
Num of Instance Load :           1

...Omitted contents

```

- 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
-----
OsUrl          : 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

```

---

■ **Verifying the Flash Media Streaming Engine**



## Specifications and Part Numbers

This appendix provides software license information related to the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS).

- [Application License, page K-1](#)
- [Advanced Feature License, page K-1](#)
- [Capacity License, page K-2](#)
- [Other Licenses, page K-2](#)

## Application License

The tables in this section list the Purchased PIDs available for the Cisco VDS-IS.

**Table K-1 Application License Options**

PID	Description
VDSIS-CDEAPPS-K9	Multi-Protocol Streamer Software Apps Appliance License
VDSMU-K9	Multi-Protocol (HTTP, RTSP, RTMP) Streamer + 1 Gbps Capacity
VDSHU-K9	HTTP Streamer + 1 Gbps Capacity + Acquirer Function
VDSSR-K9	Service Router License + 100 TPS
VDSMGR-K9	VDS Manager/CDSM
R-VDSISBUUL	VDS-IS Bundle for Redundant Element Management, Service Routing, CDN Analytics
R-VDSISBU20	VDS-IS Bundle for Redundant Element Management Limited to 20 Streamers, Service Routing
R-VDSISBU-UPGR	Upgrade to R-VDSISBUUL=. Requires either R-VDSISBU20=, or 2 x VDSMGR-K9 and 2 x VDSSR-K9
VDSMULO-K9	Multi-Protocol Streamer License + 200 Mbps Capacity

## Advanced Feature License

The tables in this section list the Advanced feature license options available for the Cisco VDS-IS.

**Table K-2 Advance Feature License Options**

<b>PID</b>	<b>Description</b>
VDSURL	URL Signing Feature License, per Streamer
VDSSBE	HTTP Session Based Encryption License, per Streamer
VDSHSL	HTTPS Secure Delivery License, per Streamer
VDSMCR	Multicast Receiver License, per Streamer
VDSMCS	Multicast Sender License, per Sender
VDSQTA	SR - Session and Bandwidth Quota Enforcement

## Capacity License

The tables in this section list the Capacity license options available for the Cisco VDS-IS.

**Table K-3 Capacity License Options**

<b>PID</b>	<b>Description</b>
L-VDSHT1	Tier 1 (0 - 50 GBps) HTTP Delivery, per Gbps
L-VDSHT2	Tier 2 (51 - 250 GBps) HTTP Delivery, per Gbps
L-VDSHT3	Tier 3 (250 1000GBps) HTTP Delivery, per Gbps
L-VDSMT1	Tier 1 (0 - 50 GBps) Multi-Protocol Delivery, per Gbps
L-VDSMT2	Tier 2 (51 - 250 GBps) Multi-Protocol Delivery, per Gbps
L-VDSMT3	Tier 3 (250 - 1000GBps) Multi-Protocol Delivery, per Gbps
L-VDSHTSUB	Annual Subscription, HTTP Delivery, per Gbps
L-VDSMTSUB	Annual Subscription, Multi-Protocol Delivery, per Gbps
L-VDSPSE150	VDS-IS Service Router - Enhanced Proximity Services, 150TPS
L-VDSSR500	500 TPS Server Router Upgrade

## Other Licenses

The tables in this section list the other license options available for the Cisco VDS-IS.

**Table K-4 Other License Options**

<b>PID</b>	<b>Description</b>
VDSMU-3-UPGR	Upgrade Streamer from 2.x to 3.x
VDSSR-3-UPGR	Upgrade Service Router from 2.x to 3.x
VDSMGR-3-UPGR	Upgrade Manager from 2.x to 3.x

**Table K-4      Other License Options (continued)**

PID	Description
CDA-VDSMU-3.0	Multi-Protocol Streamer License for 3.0 release
CDA-VDSMU-4.0	Multi-Protocol Streamer License for 4.0 release

■ **Other Licenses**