CHAPTER 5

Configuring Services

This chapter provides information on configuring the CDS. This chapter covers the following major topics:

- Configuring Delivery Services, page 5-1
- Configuring Programs, page 5-26
- Viewing Programs, page 5-39
- Copying a Program, page 5-41

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
- Creating Delivery Service
- Identifying Content

Content Origins

Content is stored on origin servers. Each delivery service is configured with one origin server. The same origin server can be used by multiple live delivery services. However, only one prefetch/caching delivery service is allowed per origin server.

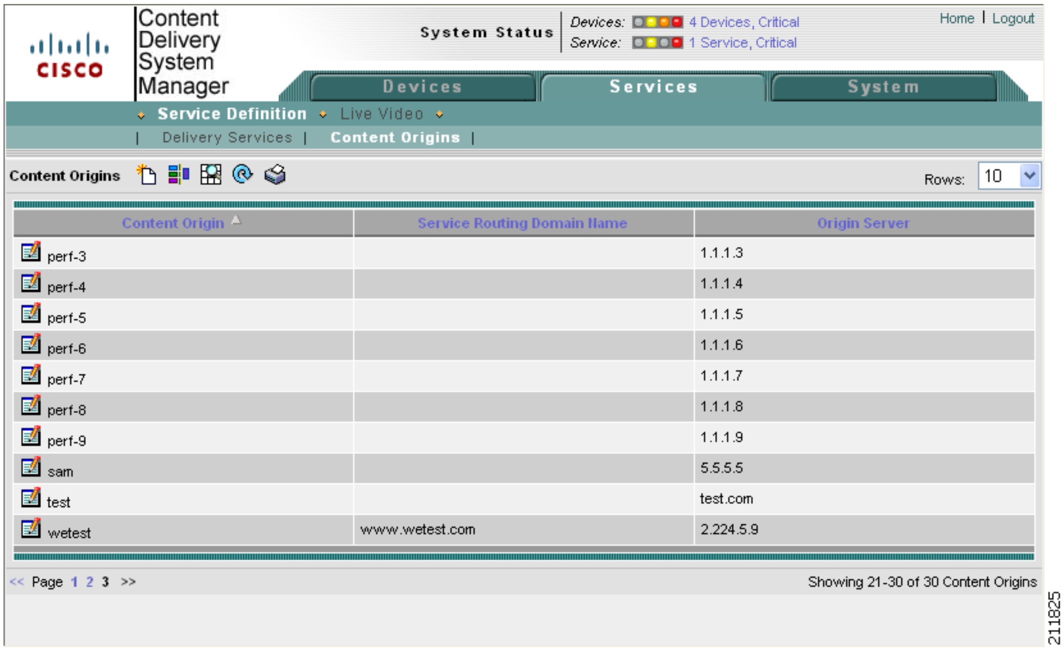
Note When creating a live delivery service with the same Content Origin as a prefetch/caching delivery service, the same set of SEs must be assigned to both; otherwise, the SR may redirect requests to unassigned SEs.

For more information about origin servers, see the "Origin Servers" section on page 2-5.

To create a Content Origin, do the following:

Step 1 Choose **Services > Service Definition > Content Origins**. The Content Origin Table page is displayed (Figure 5-1).

Figure 5-1 Content Origin Table Page

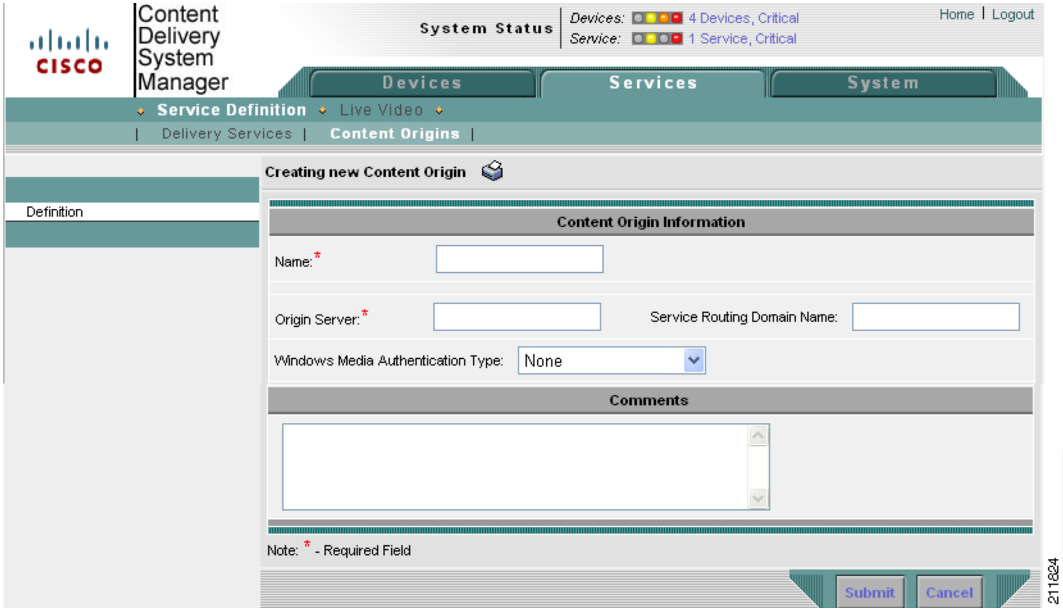


Content Origin	Service Routing Domain Name	Origin Server
perf-3		1.1.1.3
perf-4		1.1.1.4
perf-5		1.1.1.5
perf-6		1.1.1.6
perf-7		1.1.1.7
perf-8		1.1.1.8
perf-9		1.1.1.9
sam		5.5.5.5
test		test.com
wetest	www.wetest.com	2.224.5.9

<< Page 1 2 3 >> Showing 21-30 of 30 Content Origins

Step 2 Click the **Create New** icon in the task bar. The Content Origin page is displayed (Figure 5-2).

Figure 5-2 Content Origin Page



Creating new Content Origin

Content Origin Information

Name:*

Origin Server:*

Service Routing Domain Name:

Windows Media Authentication Type: None

Comments

Note: * - Required Field

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	Fully qualified domain name (FQDN) of the origin server.
Service Routing Domain Name	The FQDN to route client requests. The SE translates the service routing domain name (SRDN) to the origin server whenever it needs to retrieve content from the origin server. The service routing domain name configured for the Content Origin should also be configured in the DNS servers, so client requests can get redirected to a Service Router for request mediation and redirection. The URLs that are published to the users have the service routing domain names as the prefix.
Windows Media Authentication Type	The type of client authentication that is required by the origin server. The options are: • None • Basic authentication • NTLM authentication • Digest\ • Negotiate
Comments	Information about the Content Origin.

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 you want to delete, and click the **Trash** icon in the task bar.

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 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:

1. Service Definition
2. SE and Content Acquirer Assignment or Device Group and Content Acquirer Assignment
3. PCMM Configuration
4. General Settings
5. Session Shifting
6. Identifying Content

Configuring the first five are described in the following procedure. Identifying content is described in the "Identifying Content" section on page 5-11.

Tip For information about testing a delivery service, see Appendix G, "Testing the Internet Streamer CDS."

To create a delivery service, do the following:

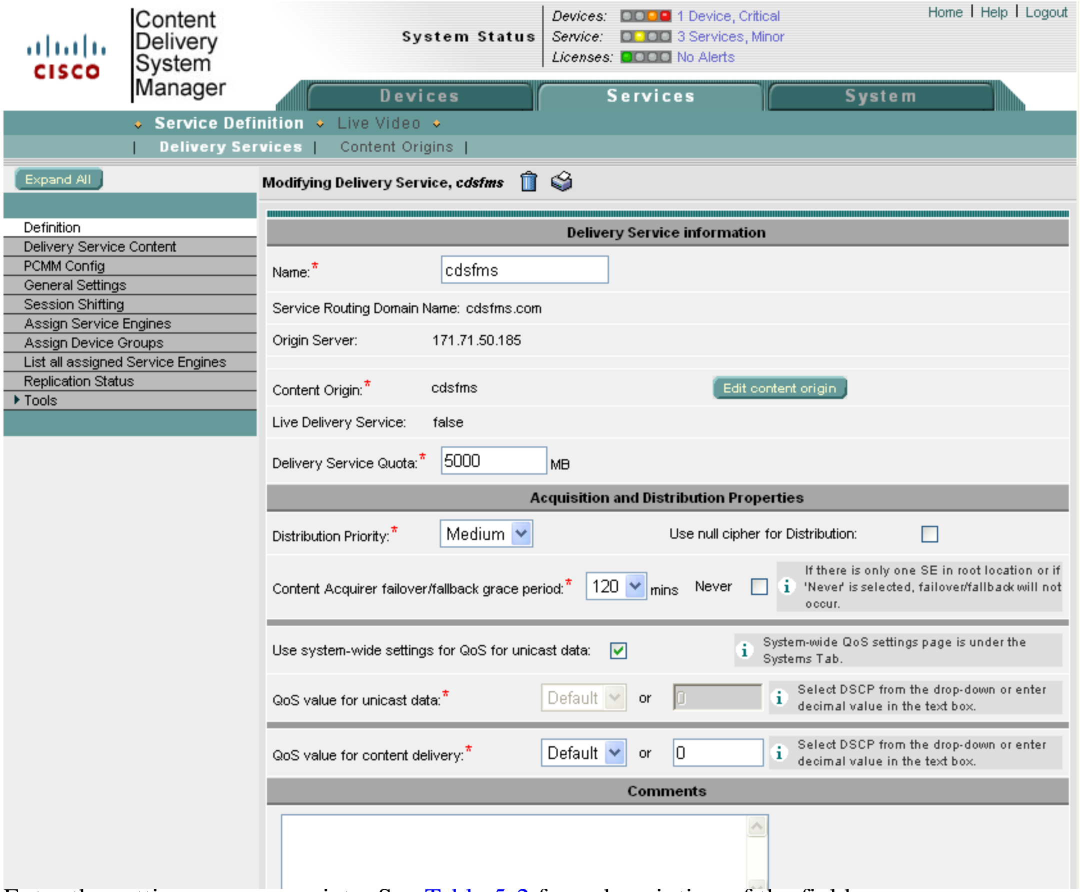
Service Definition

Step 1 Choose **Services > Service Definition > Delivery Services**. The Delivery Services Table page is displayed (Figure 5-3).

Step 2 Click the **Create New** icon in the task bar. The Delivery Services Definition page is displayed (Figure 5-3).

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

Figure 5-3 ***Delivery Service Definition Page***



Devices: 1 Device, Critical
Service: 3 Services, Minor
Licenses: No Alerts

Modifying Delivery Service, *cdsfms*

Delivery Service information

Name:* cdsfms

Service Routing Domain Name: cdsfms.com

Origin Server: 171.71.50.185

Content Origin:* cdsfms

Live Delivery Service: false

Delivery Service Quota:* 5000 MB

Acquisition and Distribution Properties

Distribution Priority:* Medium

Use null cipher for Distribution: □

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 0 Select DSCP from the drop-down or enter decimal value in the text box.

QoS value for content delivery:* Default or 0 Select DSCP from the drop-down or enter decimal value in the text box.

Comments

Step 3 Enter the settings as appropriate. See Table 5-2 for a description of the fields.

Table 5-2 ***Delivery Service Definition Fields***

Field	**Description**
Delivery Service Information	
Name	Unique name for the delivery service.
Content Origin	All Content Origins that have been created are listed in the drop-down list. The delivery service and the Content Origin have a one-to-one relationship. To create a new Content Origin, click **New Content Origin**.
Live Delivery Service	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. Checking this check box disables the Delivery Service Quota field and fields in the Acquisition and Distribution Properties section.
Delivery Service Quota	Maximum content storage size, in megabytes, for prefetched, hybrid, or, cached content for this delivery service.

Table 5-2 Delivery Service Definition Fields (continued)

Field	Description
Acquisition and Distribution Properties	
Distribution Priority	Content distribution priority setting. Options are High, Normal, and Low. The default is Normal. 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.
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 1-27.
Never	When checked, SE failover or fallback never occurs.
Use system-wide settings for QoS for unicast data	When checked, applies the system-wide QoS settings for unicast data to the delivery service. 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.
QoS value for unicast data	Configures a Differentiated Services Code Point (DSCP) value for the QoS. If you choose **Other**, enter a decimal value in the corresponding field. 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.
QoS value for content delivery	Configures a Differentiated Services Code Point (DSCP) value for the QoS on a per-delivery service basis. If you choose **Other**, enter a decimal value in the corresponding field. **Note** This is a Release 2.3 feature and applies only to Windows Media Stream Streaming and Web engines.
Comments	Information about the delivery service.

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

To delete a delivery service, from the Delivery Service Table page, click the **Edit** icon next to the delivery service you want to delete, and click the **Trash** icon in the task bar.

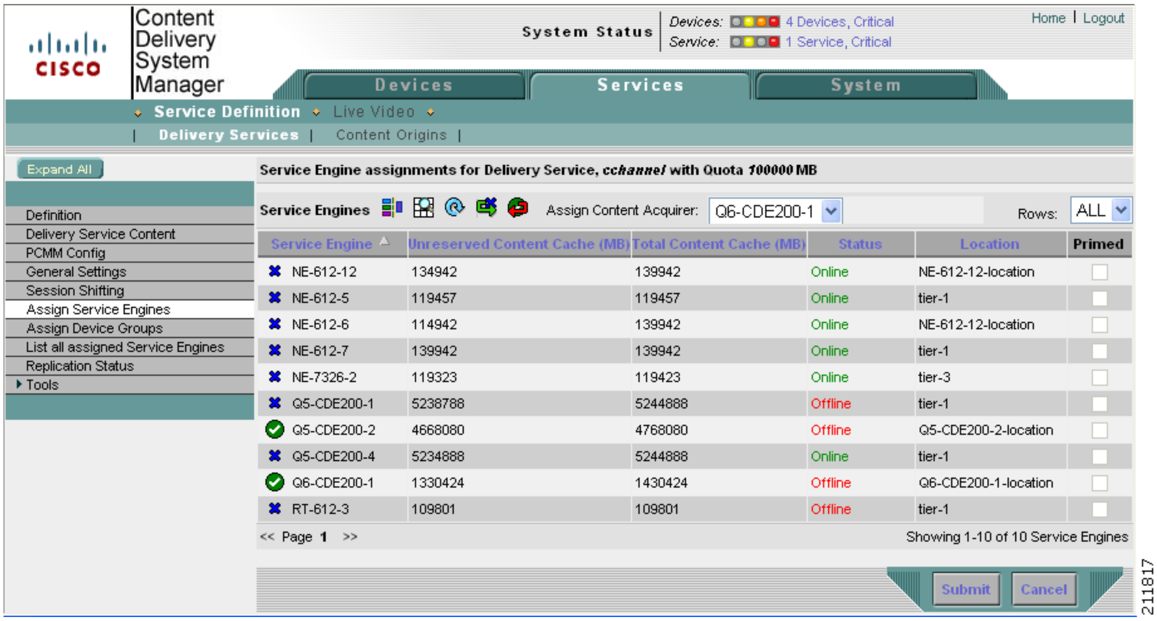
SE and Content Acquirer Assignment or Device Group and Content Acquirer Assignment

Step 5 through Step 8 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 5 through Step 8 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 5 From the left-panel menu, click **Assign Service Engines**. The Service Engine Assignment page is displayed (Figure 5-4).

Figure 5-4 Service Engine Assignment Page



Content Delivery System Manager

System Status Devices: 4 Devices, Critical Service: 1 Service, Critical

Home | Logout

Devices | Services | System

Service Definition | Live Video

Delivery Services | Content Origins

Expand All

- Definition
- Delivery Service Content
- PCMM Config
- General Settings
- Session Shifting
- Assign Service Engines
- Assign Device Groups
- List all assigned Service Engines
- Replication Status
- Tools

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	☐
✖ NE-612-5	119457	119457	Online	tier-1	☐
✖ NE-612-6	114942	139942	Online	NE-612-12-location	☐
✖ NE-612-7	139942	139942	Online	tier-1	☐
✖ NE-7326-2	119323	119423	Online	tier-3	☐
✖ Q5-CDE200-1	5238788	5244888	Offline	tier-1	☐
✓ Q5-CDE200-2	4668080	4768080	Offline	Q5-CDE200-2-location	☐
✖ Q5-CDE200-4	5234888	5244888	Online	tier-1	☐
✓ Q6-CDE200-1	1330424	1430424	Offline	Q6-CDE200-1-location	☐
✖ RT-612-3	109801	109801	Offline	tier-1	☐

<< Page 1 >>

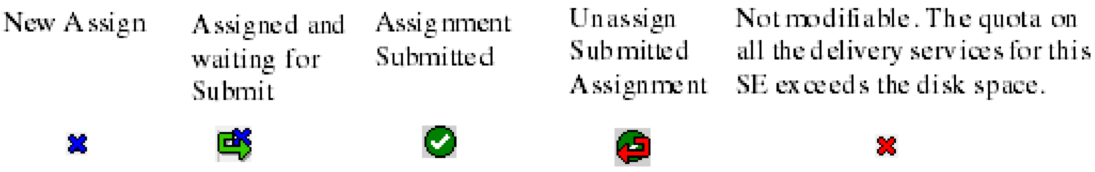
Showing 1-10 of 10 Service Engines

Submit Cancel

211817

Step 6 Click the **Assign** icon (blue cross mark) next to the SE you want to assign to this delivery service. Alternatively, in the task bar, click **Assign All Service Engines**. The SE assignment states are described in Figure 5-5.

Figure 5-5 SE Assignment States


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 7 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 5-34.

Step 8 Click **Submit** to save the SE and Content Acquirer assignments.

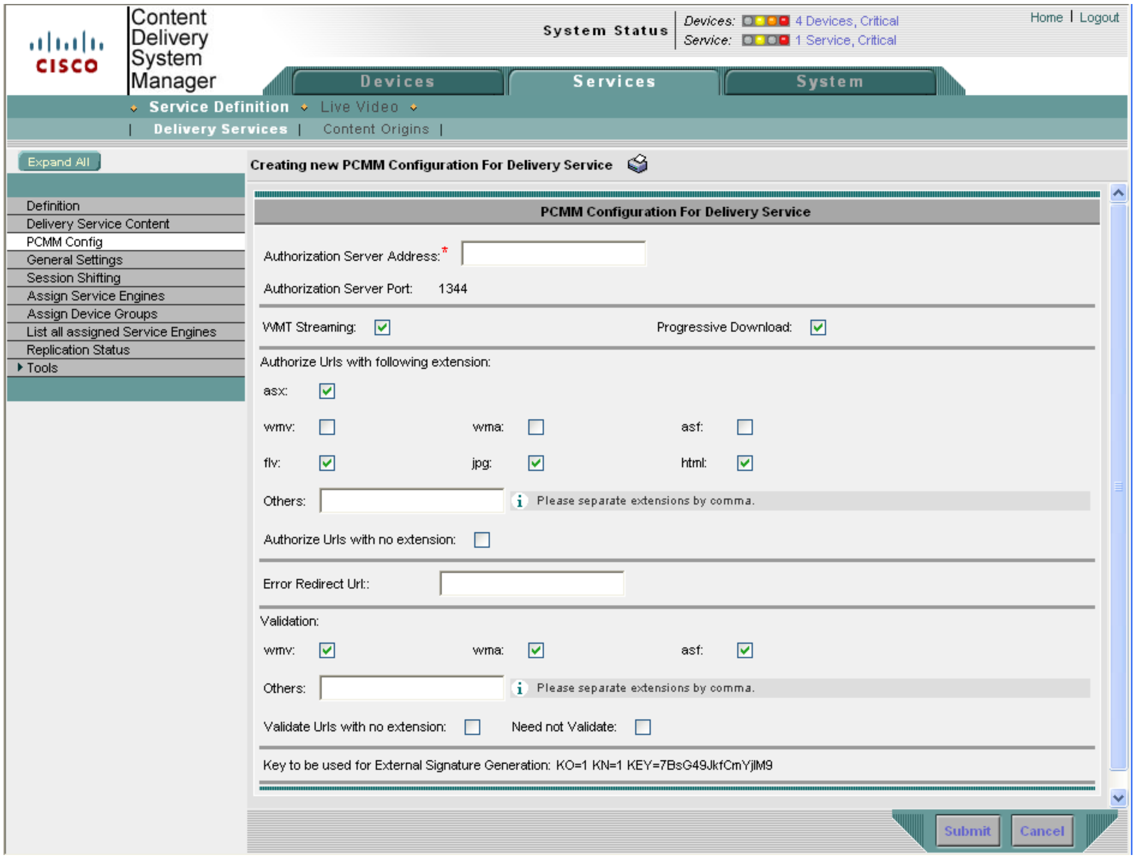
A green circle with a check mark indicates an SE is assigned to this delivery service. To unassign the SE, click this icon, or click **Unassign All Service Engines** in the task bar. Click **Submit** to save the changes.

Note To view all the Service Engines assigned to the delivery service, in the left-panel menu, click **List assigned Service Engines**.

PCMM Configuration

Step 9 From the left-panel menu, click **PCMM Config**. The PCMM Configuration page is displayed (Figure 5-6).

Figure 5-6 PCMM Configuration Page



Creating new PCMM Configuration For Delivery Service

PCMM Configuration For Delivery Service

Authorization Server Address:*

Authorization Server Port: 1344

WMT Streaming: ☑ Progressive Download: ☑

Authorize Urls with following extension:

asx: ☑

wmv: □ wma: □ asf: □

flv: ☑ jpg: ☑ html: ☑

Others: Please separate extensions by comma.

Authorize Urls with no extension: □

Error Redirect Url::

Validation:

wmv: ☑ wma: ☑ asf: ☑

Others: Please separate extensions by comma.

Validate Urls with no extension: □ Need not Validate: □

Key to be used for External Signature Generation: KO=1 KN=1 KEY=7BsG49JkfCmYjlM9

Step 10 Enter the settings as appropriate. See Table 5-3 for a description of the fields.

Table 5-3 PCMM Configuration Fields

Field	Description
Authorization Server Address	The IP address of the policy server.
Authorization Server Port (read only)	The port the policy server listens on for incoming authorization requests.

Table 5-3 PCMM Configuration Fields (continued)

Field	Description
WMT Streaming	When checked, an HTTP callout to the policy server is done for each stream request.
Progressive Download	When checked, an HTTP callout to the policy server is done for each download request.
Authorize URLs with following extensions	All URLs with file extensions that match those checked, or specified in the **Others** field (comma-separated), are authorized using ICAP.
Authorize URLs with no extensions	When checked, all URLs with no file extensions are authorized using ICAP.
Error Redirect URL	If the URL authorization fails, the request is redirected to the error URL specified in the field.
Validation	All URLs with file extensions that match those checked, or specified in the **Others** field (comma-separated), are validated in the SE.
Validation URLs with no extension	When checked, all URLs with no file extensions are validated in the SE.
Need not validate	When checked, validation is turned off.
Key to be used for External Signature Generation (Informational only)	The CDSM displays: `KO=1 KN=1 KEY=yEOCA6C7TWh4NAw9.` where • KO is the signature key owner. • KN is the signature key number. For information about configuring URL key signatures, see the "Configuring URL Signing" section on page 4-23.

Step 11 Click **Submit** to save the settings.

General Settings

Step 12 From the left-panel menu, click **General Settings**. The General Settings page is displayed.

Step 13 In the **Maximum Bitrate Limit per Session for HTTP** field, enter the maximum rate, in Kbps, at which a client can receive content.

This bit rate applies to content that is stored locally, specifically, prefetched, hybrid, or cached. For a cache miss, content is delivered at the rate the origin server sends it.

Step 14 In the **Maximum Bitrate Limit per Session for HTTP Cache Miss** field, enter the maximum rate, in Kbps, at which a client can receive content that was a cache miss.

This bit rate applies to content that is not stored locally, specifically, content requiring dynamic caching from the origin server or another SE in the delivery service that has the content.

Note This is a Release 2.1 feature.

Step 15 In the **Disable HTTP Download** field, check the check box to not allow clients to download HTTP content through this delivery service.

This option disables all HTTP-based content serving from this delivery service. The Web Engine will return a 403 forbidden message.

Note 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. This is a Release 2.1 feature.

Step 16 Check the **Enable streaming over HTTP** check box and specify the file types in the **HTTP Allowed Extensions** field to configure progressive download or streaming for certain media files. This setting applies only to the following file types: .asf, none, .nsc, .wma, .wmv, and nsclog.

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.

Note This is a Release 2.3 feature.

Step 17 Click **Submit** to save the settings.

Session Shifting

For more information on session shifting, see the "3-Screen Session Shifting" section on page 1-5.

Note 3-Screen Session Shifting is a Release 2.2 feature and supports RTSP streaming for the Windows Media and Movie Streamer engines.

Step 18 From the left-panel menu, click **Session Shifting**. The Session Shifting page is displayed.

Step 19 Enter the settings as appropriate. See Table 5-4 for a description of the fields.

Table 5-4 Session Shifting Fields

Field	Description
Enable	When enabled, session shifting interoperates with the TV CDS.
TV-Streamer IP	The IP address of the TV Streamer participating in session shifting.
TV-Streamer Port	The port of the TV Streamer participating in session shifting.
Service Router	The Service Router that is designated as the centralized session manager. Only one Service Router is used for all session shifting delivery services. The same Service Router must be designated as the centralized session manager for all delivery services that use session shifting.

Table 5-4 Session Shifting Fields (continued)

Field	Description
Content File Subscriber File Profile File	For each session shifting file, click the **Browse** button to locate each XML file. The Choose File dialog box is displayed. Navigate to the file and click **Open**. To remove a file, click the **Trash** icon next to the file type. To view the file, click **List**. For more information on the session shifting XML files, see Appendix D, "Creating and Manipulating Session Shifting Files."

Step 20 Click **Submit** to save the settings.

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.

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.

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 will search 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.

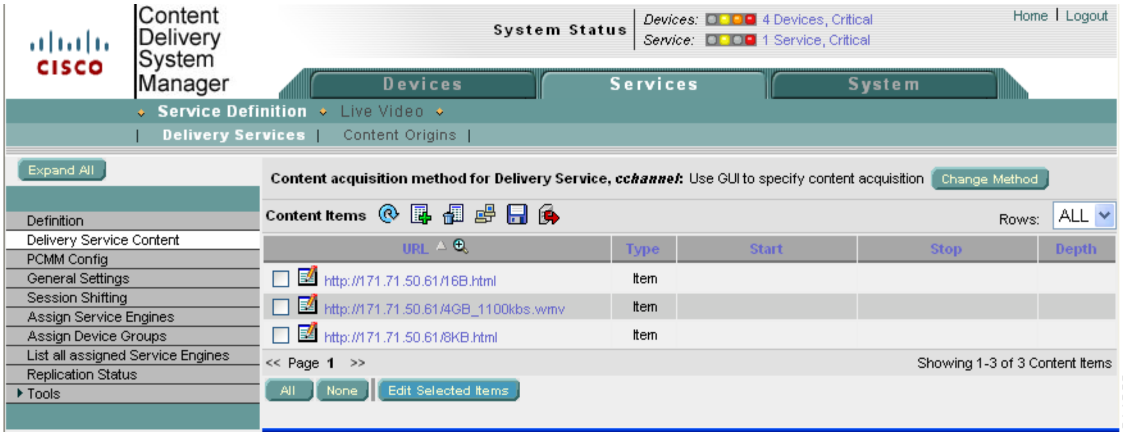
- Select individual items by performing a quick crawl, and select the items from the crawl result list to be included in the content list.

For more information about the crawler feature, see the "Crawling" section on page 2-5.

To identify content for acquisition using the CDSM, do the following:

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 5-7).

Figure 5-7 Content Table Page



Content acquisition method for Delivery Service, *cchannel*: Use GUI to specify content acquisition

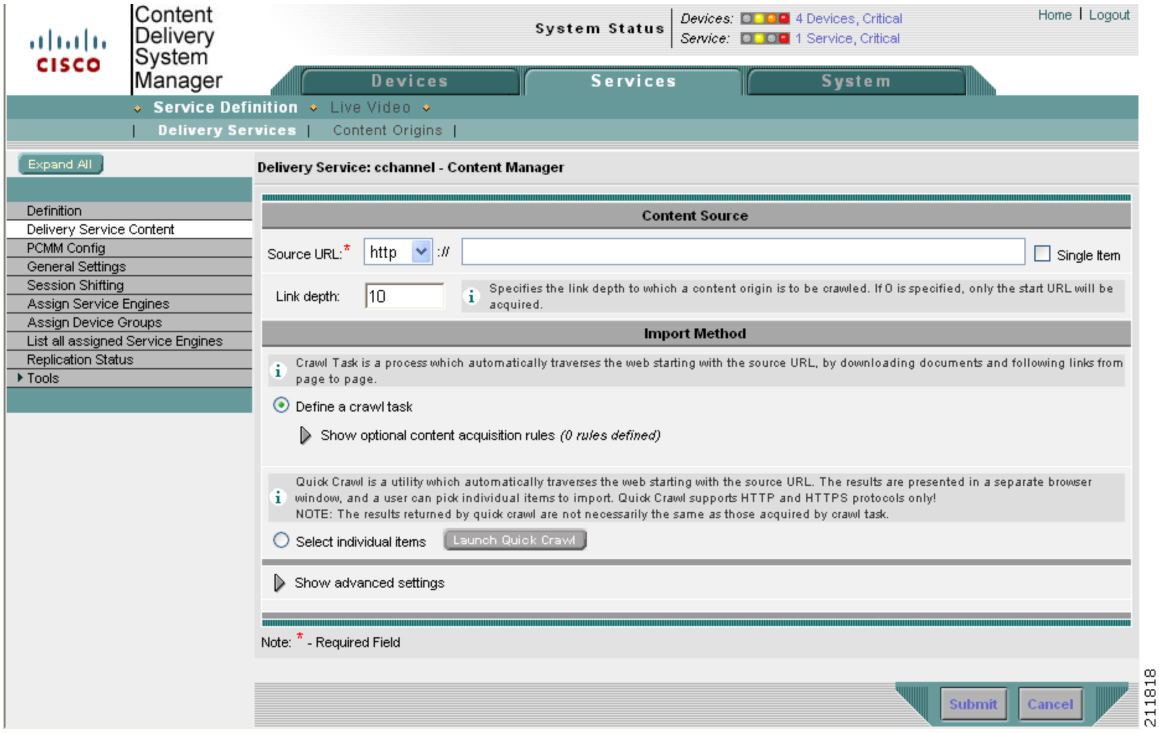
	URL	Type	Start	Stop	Depth
□	http://171.71.50.61/16B.html	Item			
□	http://171.71.50.61/4GB_1100kbs.wmv	Item			
□	http://171.71.50.61/8KB.html	Item			

<< Page 1 >> Showing 1-3 of 3 Content Items

211822

Step 2 Click the **Add Content** icon in the task bar. The Content Manager page is displayed (Figure 5-8).

Figure 5-8 Content Manager Page



Delivery Service: cchannel - Content Manager

Content Source

Source URL:* http :// □ Single Item

Link depth: 10

Specifies the link depth to which a content origin is to be crawled. If 0 is specified, only the start URL will be acquired.

Import Method

Crawl Task is a process which automatically traverses the web starting with the source URL, by downloading documents and following links from page to page.

● Define a crawl task

Show optional content acquisition rules *(0 rules defined)*

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.

○ Select individual items

Show advanced settings

Note: * - Required Field

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 5-21.

Step 3 Choose a protocol from the **Source URL** drop-down list, and enter the source URL in the associated field.

The source URL is the origin server domain name or IP address, followed by a path, or path and filename, if applicable.

Note The URL format for Server Message Block (SMB) servers is: \\SMB server:port\sharedfolder\filepath. If port is not specified in the URL, the default port, 139, is used. Maximum file size, when using SMB for acquisition, is 2 GB. Symbolic links within exported file systems (SMB or NFS) must contain a relative path to the target file, or the target file should be copied into the exported volume.

Step 4 Do one of the following:

a. To identify a single content item, check the **Single Item** check box, and go to the "Configuring Advanced Settings" section on page 5-17 in this procedure.

b. To define a crawl, uncheck the **Single Item** check box, and in the **Link Depth** field, enter the depth of the links to search. Go to the "Defining a Crawl Task" section on page 5-14 in this procedure.

c. To perform a quick crawl, uncheck the **Single Item** check box, and, in the **Link Depth** field, enter the depth of the links to search. Go to the "Launching Quick Crawl" section on page 5-16 in this procedure.

The crawler feature starts with the Source URL, identifies every web link in the page, and adds every link to the list of URLs to search, until the links have been followed to the specified depth.

The Link Depth field specifies how many levels of a website to crawl or how many directory levels of an FTP server to search. This is optional. The range is –1 to 2147483636.

If the depth is –1, there is no depth constraint.

If the depth is 0, content is acquired only at the starting URL.

If the depth is 1, content is acquired starting at the URL and includes content the URL references.

Defining a Crawl Task

To define a crawl task, do the following:

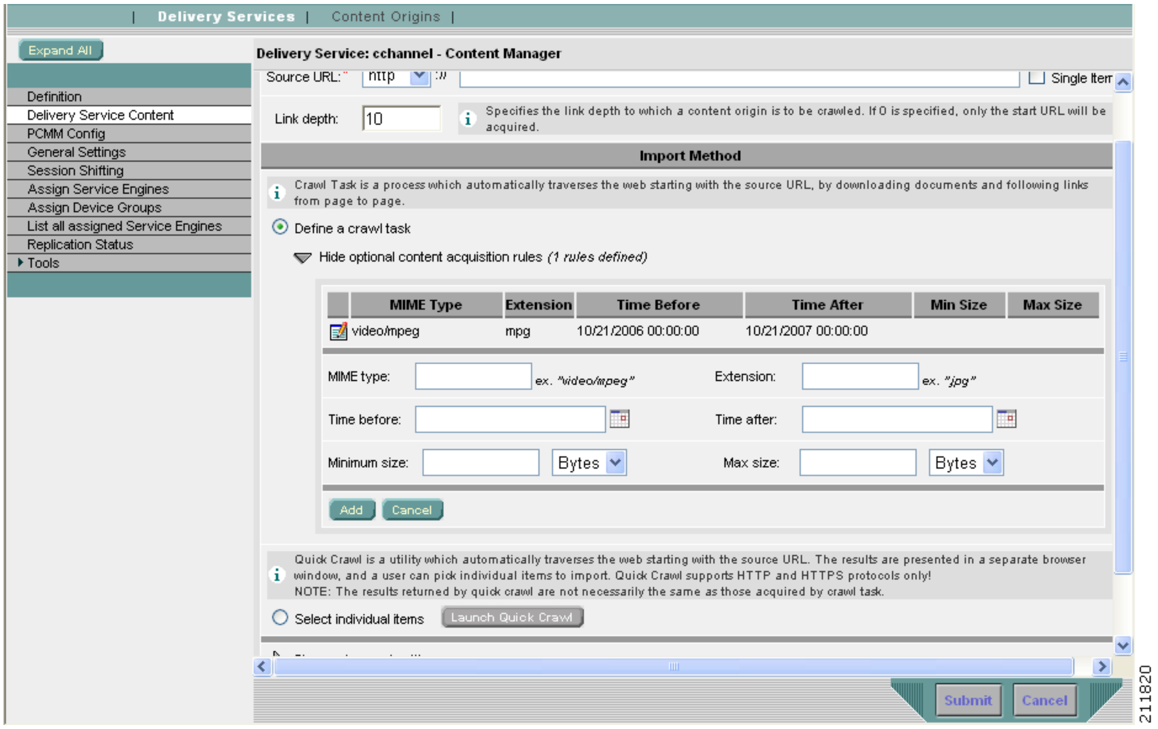
Step 1 Click the **Define a Crawl Task** radio button.

Step 2 Do *one* of the following:

- **a.** Click **Submit** (or **Update** if you are editing an existing content) to add a crawl task to the delivery service. The local Manifest file is automatically reparsed, changes are detected, and the corresponding content items are acquired or removed.
- **b.** Go to the "Configuring Advanced Settings" section on page 5-17, if applicable.
- **c.** 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 5-9), and the arrow becomes the **Hide Optional Content Acquisition Rules** arrow.

Figure 5-9 Content Manager Page—Acquisition Rules Fields



Delivery Service: cchannel - Content Manager

Source URL:* http :// □ Single Item

Link depth: 10

Specifies the link depth to which a content origin is to be crawled. If 0 is specified, only the start URL will be acquired.

Import Method

Crawl Task is a process which automatically traverses the web starting with the source URL, by downloading documents and following links from page to page.

● Define a crawl task

Hide optional content acquisition rules *(1 rules defined)*

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		

MIME type: ex. "video/mpeg" Extension: ex. "jpg"

Time before: Time after:

Minimum size: Bytes Max size: Bytes

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.

○ Select individual items

Step 4 Enter the settings as appropriate. See Table 5-5 for a description of the fields.

Table 5-5 Acquisition Rule Fields

Field	Description
MIME Type	A content item qualifies for acquisition only if its MIME type matches this MIME type (for example, video/mpeg).
Extension	A content item is acquired only if its extension matches this extension.
Time Before	Files that were modified before this time qualify for acquisition. Use the dd-mm-yyyy hh:mm:ss [TMZ] format, where TMZ (the time zone) is optional. UTC is the default. Alternatively, click the **Calendar** icon to choose a date from the calendar and enter a time, and click **Apply**.
Time After	Files that were modified after this time qualify for acquisition. Use the format dd-mm-yyyy hh:mm:ss [TMZ] format, where TMZ (the time zone) is optional. UTC is the default. Alternatively, click the **Calendar** icon to choose a date from the calendar and enter a time, and click **Apply**.
Minimum Size	Content equal to or larger than this value qualifies for acquisition. Choose **MB**, **KB**, or **Bytes** 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 **MB**, **KB**, or **Bytes** as the unit of measure. The range is 0 to 2147483636.

Step 5 Click **Add** to add the rule to the rules list. An entry is added showing the values under each column heading.

Note A maximum of ten rules can be configured for each crawl task.

To modify a content acquisition rule, click the **Edit** icon next to the rule. Once you have finished, click the small **Update** button in the content acquisition rules section to save the edits.

To delete a content acquisition rule, click the **Edit** icon next to the rule. Click the **Delete** button in the content acquisition rules section. The rule is removed from the rules listing.

Step 6 When you have finished adding and modifying content acquisition rules, do one of the following:

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 5-17, 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, do the following:

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 5-6 for a description of the fields.

Table 5-6 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 **Calendar** 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 **Calendar** 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 **MB**, **KB**, or **Bytes** 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 **MB**, **KB**, or **Bytes** 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.

Table 5-6 Quick Crawl Filter Fields (continued)

Field	Description
Max Item Count	The maximum number of content items that is listed in the results. The maximum value is 1000.
Domain	The *host.domain* 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 being search. The Searching for Content status displays a progress bar and shows the number of items found.

Click **Show Results** to display the content items before the search is complete.

Click **Refresh Results** to refresh the progress bar.

When finished, the search results list the MIME type, size, date modified, and URL of each content item that met the search criteria.

Step 4 Check the check box next to the content items you want to include in this delivery service. Use the **Row** drop-down list to show all content items, or use the **Page** option at the bottom of the table to go to the next page.

Alternatively, click **Select All** to select all content items. To deselect all, click **Select None**.

Step 5 Click **Add Selected** to add all selected content items to the delivery service. The Content Table page is displayed with all the selected content items listed.

Click **Show Filter** to return to the filter and change the filter settings.

Step 6 To configure advanced settings for the content items listed, click **All** at the bottom of the Content Table page, and then click **Edit Selected Items**. The Content Manager page is displayed with the Advanced Settings option.

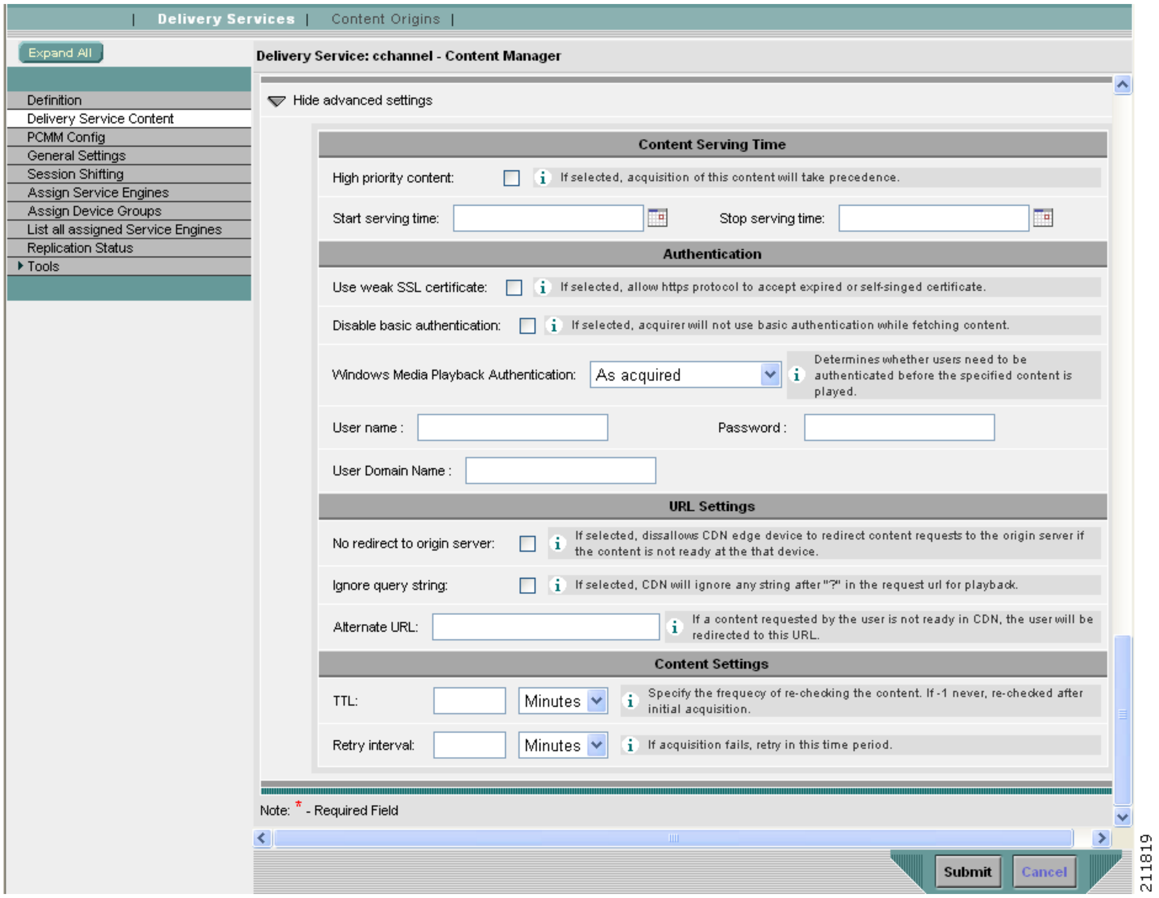
Configuring Advanced Settings

Advanced settings offer controls on how the content is delivered to the client devices.

To configure the advanced settings, do the following:

Step 1 Click the **Show Advanced Settings** arrow. The Advanced Settings fields are displayed (Figure 5-10), and the arrow becomes the **Hide Advanced Settings** arrow.

Figure 5-10 Content Manager Page—Advanced Settings Fields



| Delivery Services | Content Origins |

Expand All

Delivery Service: cchannel - Content Manager

- Definition
- Delivery Service Content
- PCMM Config
- General Settings
- Session Shifting
- Assign Service Engines
- Assign Device Groups
- List all assigned Service Engines
- Replication Status
- Tools

Hide advanced settings

Content Serving Time

High priority content: □ If selected, acquisition of this content will take precedence.

Start serving time: Stop serving time:

Authentication

Use weak SSL certificate: □ If selected, allow https protocol to accept expired or self-singed certificate.

Disable basic authentication: □ If selected, acquirer will not use basic authentication while fetching content.

Windows Media Playback Authentication: As acquired — Determines whether users need to be authenticated before the specified content is played.

User name : Password :

User Domain Name :

URL Settings

No redirect to origin server: □ If selected, dissallows CDN edge device to redirect content requests to the origin server if the content is not ready at the that device.

Ignore query string: □ If selected, CDN will ignore any string after "?" in the request url for playback.

Alternate URL: If a content requested by the user is not ready in CDN, the user will be redirected to this URL.

Content Settings

TTL: Minutes — Specify the frequecy of re-checking the content. If -1 never, re-checked after initial acquisition.

Retry interval: Minutes — If acquisition fails, retry in this time period.

Note: * - Required Field

Submit Cancel

Step 2 Enter the settings as appropriate. See Table 5-7 for a description of the fields.

Table 5-7 Advanced Settings for Serving Content

Field	Description
Content Serving Time	
High Priority Content	Specifies the importance, and therefore the processing order, of the item acquisition or crawl task.
Start Serving Time	Specifies the time for the SE to start delivering content. Use the format dd-mm-yyyy hh:mm:ss [TMZ] format, where TMZ (the time zone) is optional. UTC is the default. Alternatively, click the **Calendar** icon to choose a date from the calendar and enter a time, and click **Apply**. 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.

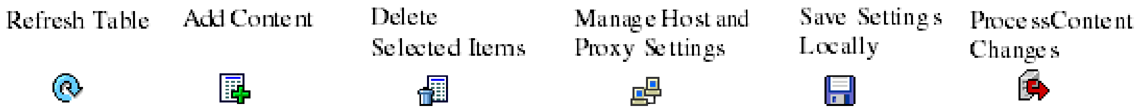
Table 5-7 Advanced Settings for Serving Content (continued)

Field	Description
Stop Serving Time	Specifies the time for the SE to stop delivering content. Use the dd-mm-yyyy hh:mm:ss [TMZ] format, where TMZ (the time zone) is optional. UTC is the default. Alternatively, click the **Calendar** icon to choose a date from the calendar and enter a time, and click **Apply**. 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 "Removing Content" section on page 8-28.
Authentication	
Use weak SSL certificate	If checked, allows acceptance of expired or self-signed certificates during authentication.
Disable basic authentication	If checked, NTLM headers are not stripped off that would allow fallback to the basic authentication method while acquiring content.
Windows Media Playback Authentication	Sets the authentication for Windows Media playback to one of the following: • As acquired—Requires authentication on playback based on settings from origin server. • Require authentication—Requires authentication upon playback. • No authentication—Does not require authentication upon playback.
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.
URL Settings	
No Redirect to Origin Server	**Note** For Releases 2.0 and 2.1 only. If checked, disallows redirecting content requests to the origin server. This attribute is a per-content object attribute, meaning that if the content has been removed, the redirection settings do not apply. However, if the Content Acquirer fails to acquire the content, then the settings apply.
Ignore Query String	If checked, ignores any string after the question mark (?) character in the requested URL for playback.
Alternate URL	**Note** This feature has been deprecated.
Content Settings	
TTL	Time period for revalidation of content. Select unit of measure from the drop-down list. If no TTL is entered, the content is fetched only once, and its freshness is never checked again.
Retry Interval	Time period in which the Content Acquirer can attempt to acquire the content again if the acquisition fails.

Step 3 Click **Submit** to process the content request. When you click **Submit**, the local Manifest file for this delivery service is automatically reparsed, changes are detected, and the corresponding items are acquired or removed. This action, however, does not trigger a recheck of all the content in the delivery service.

Content Table

The Content Table page (Figure 5-11) offers the following functions through the task bar:

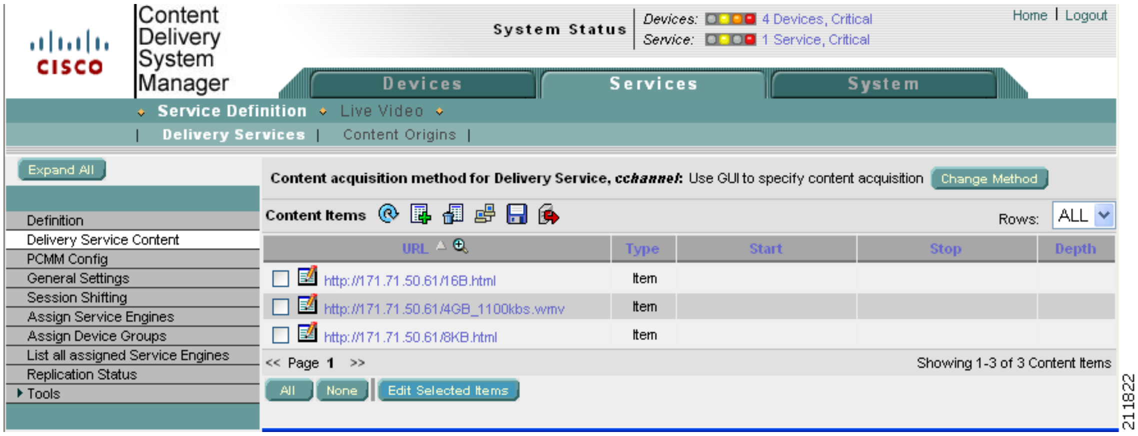


The **Refresh Table** icon refreshes the content table.

The **Add Content** icon allows you to add content items by displaying the Content Manager page.

To delete a content item, check the check box next to each item you want to delete, and click the **Delete Selected Items** icon. To select all content items, click **All**. To deselect all content items, click **None**.

Figure 5-11 Content Table Page



Content acquisition method for Delivery Service, *cchannel*: Use GUI to specify content acquisition

	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			

<< Page 1 >> Showing 1-3 of 3 Content Items

For information on the **Manage Host and Proxy Settings** icon, see the "Configuring Proxy Server Settings" section on page 5-21.

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 5-22 and Appendix B, "Creating Manifest Files."

To edit multiple content items, check the check box next to each item you want to edit, and click **Edit Selected Items**.

Configuring Proxy Server Settings

When the Content Acquirer cannot directly access the origin server, because the origin server is set up to allow access only by a specified proxy server, you can configure acquisition through a proxy server. When a proxy server is configured for the Content Acquirer, the Content Acquirer contacts the proxy server instead of the origin server, and all requests to that origin server go through the proxy server.

Note Content acquisition through a proxy server is supported only for HTTP requests.

Note Before configuring a proxy server, verify that the Content Acquirer is able to ping the proxy server. If the proxy is not servicing the configured port, you will get the message: "failed: Connection refused."

To configure a proxy server for content items identified using the CDSM, do the following:

Step 1 From the Content Table page, click the **Manage Host and Proxy Settings** icon in the task bar.

The Content Hosts Table page is displayed, listing all previously created host URLs, the number of content items for each host, and a proxy server (if configured).

To return to the Content Table page, click **Return to Content Listing**.

Step 2 Check the check box next to each host you want to configure with a proxy server.

Step 3 Click **Manage Proxy for Selected Hosts**. The Proxy Server page is displayed.

Under the Defining Proxy Server for the Following Hosts heading, a bulleted list of host servers is displayed for which proxy servers are being configured.

Step 4 In the Proxy Server Specifications area, enter the settings as appropriate. See Table 5-8 for a description of the fields.

Table 5-8 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.

Table 5-8 Proxy Server Fields (continued)

Field	Description
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-14 for more information.

To configure the Manifest file settings, do the following:

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, do the following:

a. Click **Change Method**.

b. From the drop-down list choose, **Specify external manifest file**.

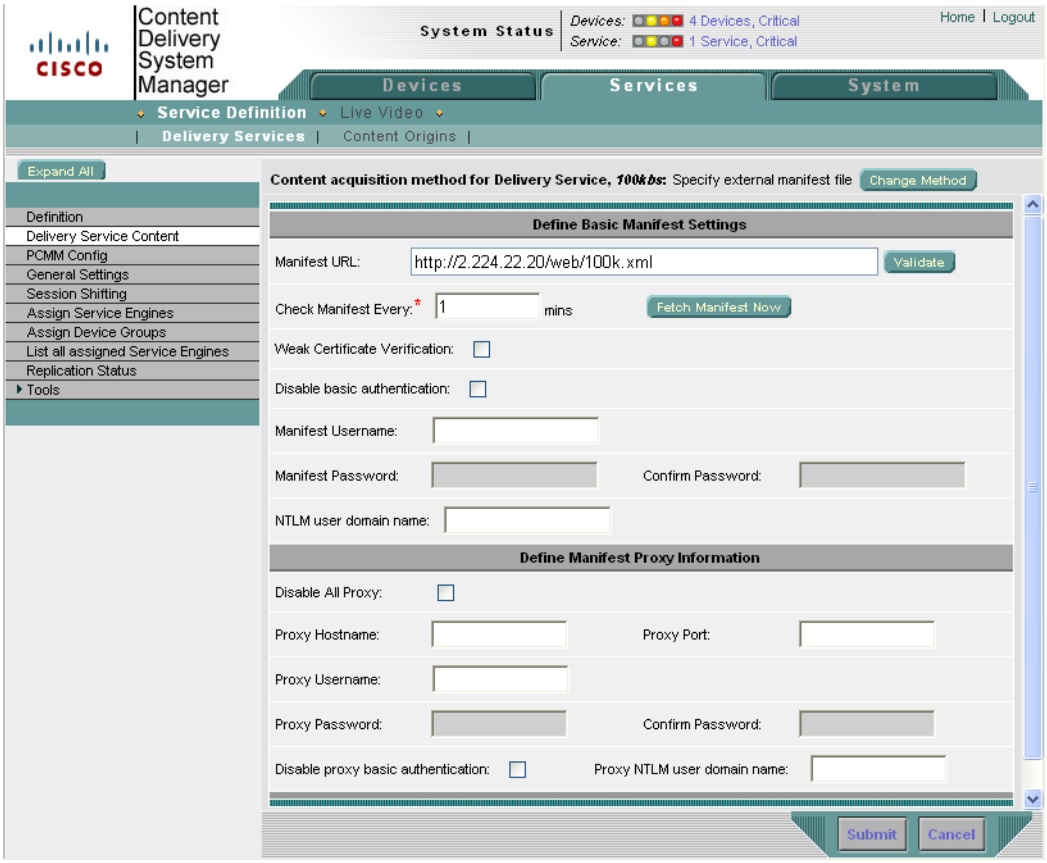
c. Click **Save**.

d. In the confirmation dialog box, click **OK**.

The Content Manager page displays the Manifest file settings (Figure 5-12).

Note When you change the content acquisition method from Use the GUI to specify content acquisition to Specify external Manifest file for an existing delivery service, any content items that you added using the CDSM are removed. To save the existing settings, click the **Save Settings Locally** icon in the task bar.

Figure 5-12 Content Manager Page—Manifest File Settings



Content acquisition method for Delivery Service, *100kbs*: Specify external manifest file

Define Basic Manifest Settings

Manifest URL: http://2.224.22.20/web/100k.xml

Check Manifest Every:* 1 mins

Weak Certificate Verification: □

Disable basic authentication: □

Manifest Username:

Manifest Password: Confirm Password:

NTLM user domain name:

Define Manifest Proxy Information

Disable All Proxy: □

Proxy Hostname: Proxy Port:

Proxy Username:

Proxy Password: Confirm Password:

Disable proxy basic authentication: □ Proxy NTLM user domain name:

211823

Step 3 Enter the settings as appropriate. See Table 5-9 for a description of the fields.

Table 5-9 Manifest File Settings Fields

Field	Description
Define Basic Manifest Settings	
Manifest URL	Address of the Manifest file for the delivery service. The Manifest URL must be a well-formed URL. If the protocol (FTP, HTTP, or HTTPS) for the URL is not specified, HTTP is used. To validate the Manifest file from this page, click **Validate**. A new window displays the validation results. For more information, see the "Manifest Validator Utility" section on page B-14.

Table 5-9 Manifest File Settings Fields (continued)

Field	Description
Check Manifest Every	Frequency in minutes (0 to 52560000) at which the Content Acquirer assigned to the delivery service checks for updates to the Manifest file. To fetch the Manifest file now, click **Fetch Manifest Now**.
Weak Certificate Verification	When checked, enables weak certificate verification for fetching the Manifest file. This is applicable when the Manifest file is fetched using HTTPS. **Note** To use weak certification for content ingest, you need to specify weak certification within the Manifest file.
Disable Basic Authentication	When checked, NTLM headers cannot be stripped off to allow fallback to the basic authentication method. If you leave this check box unchecked, NTLM authentication headers can be stripped to allow fallback to the basic authentication method, and the username and password information can be passed to the origin server in clear text with a basic authentication header.
Manifest Username	Username of the account that is allowed to fetch the Manifest file from the server. The Manifest username must be a valid ID. If the server allows anonymous login, the user ID can be null. **Note** The Manifest Username and Manifest Password fields allow you to enter any secure login information needed to access the Manifest file at its remote location.
Manifest Password	Password for the user.
Confirm Password	Password confirmation.
NTLM User Domain Name	NTLM user domain name to be allowed access by the NTLM authentication scheme configured on the server where the Manifest file is located.
Define Manifest Proxy Information	
Disable All Proxy	Disables the outgoing proxy server for fetching the Manifest file. Any outgoing proxy server configured on the Content Acquirer is bypassed, and the Content Acquirer contacts the server directly. See the "Configuring Web Engine HTTP Connections" section on page 4-43 for information about configuring outgoing HTTP proxy servers.
Proxy Hostname	Hostname or IP address of the proxy server used by the Content Acquirer to retrieve the Manifest file.
Proxy Port	Port number of the proxy sever where the Content Acquirer fetches the Manifest file. The range is from 1 to 65535.
Proxy Username	Name of the user to be authenticated to fetch the Manifest file.
Proxy Password	Password of the user to pass authentication on the proxy.
Confirm Password	Re-entry of the same password for confirmation to pass authentication on the proxy.

Table 5-9 Manifest File Settings Fields (continued)

Field	Description
Disable Proxy Basic Authentication	When checked, NTLM headers will not be stripped off to allow fallback to the basic authentication method against Microsoft Internet Information Services (IIS) servers.
Proxy NTLM User Domain Name	NTLM user domain name to be allowed access by the NTLM authentication scheme configured on the proxy.

Note When you configure a proxy server in the Manifest File Settings page, the proxy configuration is valid only for acquiring the Manifest file itself and not for acquiring the delivery service content. Requests for the Manifest file go through the proxy server, whereas requests for content go directly to the origin server.

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

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.

Configuring Programs

A program in the CDS is defined as a scheduled live or rebroadcast event that streams content to client devices. The CDS streams live or rebroadcast content by using the Movie Streamer or the Windows Media Engine. For more information, see the "Programs" section on page 2-9.

To view existing programs, see the "Viewing Programs" section on page 5-39.

Flash Media Streaming uses Real Time Media Protocol (RTMP) to stream live content by means of 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 1-18.

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 will be dropped before it reaches its destination.

Note All SEs in a Windows Media live delivery service must have Real Time Streaming Protocol with TCP (RTSPT) enabled, because SEs must use the RTSPT protocol to communicate with each other. RTSPT is enabled by default.

Tip For information about testing a live or rebroadcast program, see Appendix G, "Testing the Internet Streamer CDS."

Note The following rules apply to live splitting for Movie Streamer:

1. For unicast streaming, the client request must be sent by means of RTSP.
2. For multicast streaming, the client request must be sent by means of 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, do the following:

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.

Note The Auto Deletion check box is not supported in Release 2.1 and subsequent releases.

Step 6 In the **Description** field, enter information about the program.

Step 7 Click **Submit** to save the settings.

You have defined the type of program that you want to configure. Proceed to the section for configuring that type of program:

- To configure Movie Streamer live and Windows Media live programs, see the next section, "Configuring Live Programs."
- To configure Windows Media rebroadcast and Movie Streamer rebroadcast programs, see the "Configuring a Rebroadcast" section on page 5-34.

For information about copying a program, see the "Copying a Program" section on page 5-41.

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 5-27).

To configure a Movie Streamer live or Windows Media live program, do the following:

Step 1 After you have chosen a program from the Program Table page, click **Select Live Delivery Service**. The Select Live Delivery Service page is displayed listing all the live delivery services configured.

Step 2 Click the radio button next to the name of the live delivery service you want to associate with the program and click **Submit**. Alternatively, click the **Create New Live Delivery Service** icon in the task bar.

If you are creating a new live delivery service, the New Live Delivery Service page is displayed.

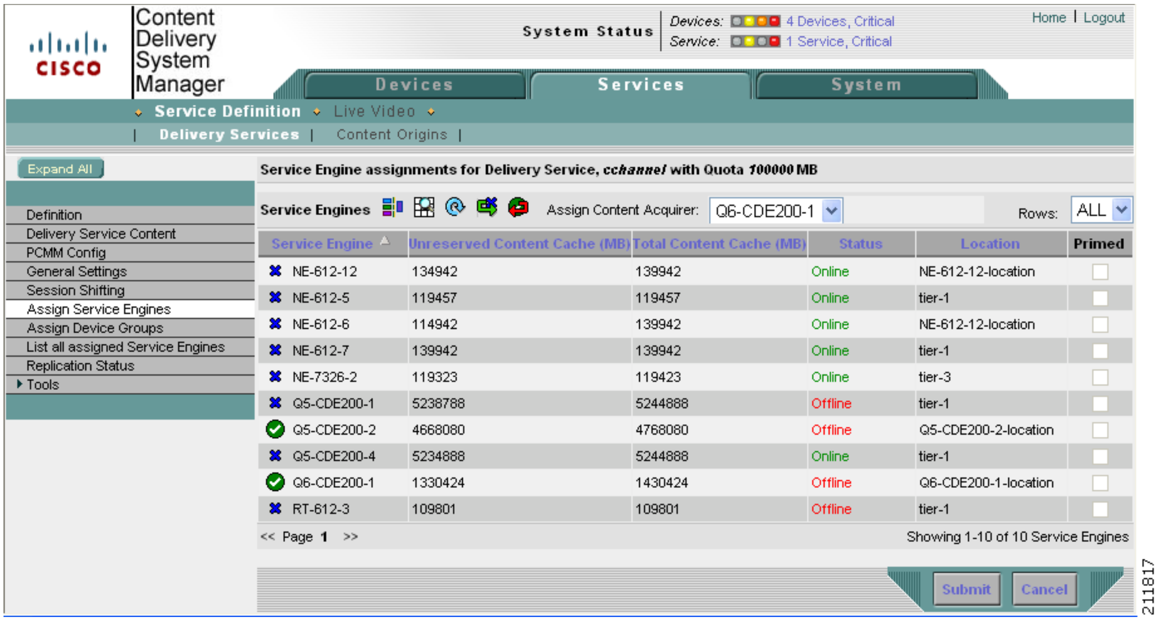
a. The **Name** field is automatically populated with a unique delivery service name. If you wish to change the name given by default, enter a unique name for the delivery service in this field.

b. From the **Content Origin** drop-down list, choose a Content Origin.

c. Click **Submit** to save the settings.

Step 3 From the left-panel menu, choose **Assign Service Engines**. The Service Engine Assignment page is displayed (Figure 5-13).

Figure 5-13 Service Engine Assignment Page



Service Engine assignments for Delivery Service, *cchannel* with Quota *100000* MB

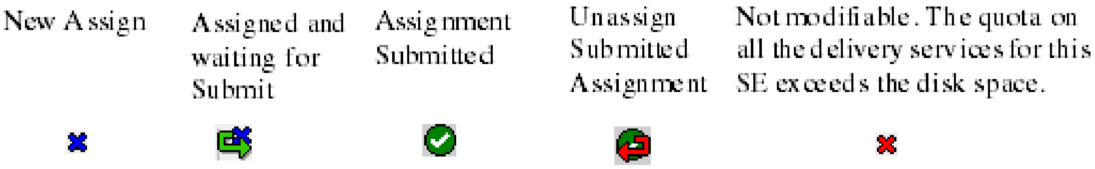
Service Engines   Assign Content Acquirer: Q6-CDE200-1   Rows: ALL

Service Engine	Unreserved Content Cache (MB)	Total Content Cache (MB)	Status	Location	Primed
✖ NE-612-12	134942	139942	Online	NE-612-12-location	□
✖ NE-612-5	119457	119457	Online	tier-1	□
✖ NE-612-6	114942	139942	Online	NE-612-12-location	□
✖ NE-612-7	139942	139942	Online	tier-1	□
✖ NE-7326-2	119323	119423	Online	tier-3	□
✖ Q5-CDE200-1	5238788	5244888	Offline	tier-1	□
✓ Q5-CDE200-2	4668080	4768080	Offline	Q5-CDE200-2-location	□
✖ Q5-CDE200-4	5234888	5244888	Online	tier-1	□
✓ Q6-CDE200-1	1330424	1430424	Offline	Q6-CDE200-1-location	□
✖ RT-612-3	109801	109801	Offline	tier-1	□

<< Page 1 >>   Showing 1-10 of 10 Service Engines

Step 4 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 5-14.

Figure 5-14 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 5 From the **Assign Content Acquirer** drop-down list in the task bar, choose an SE to be the Content Acquirer for this live delivery service.

The list contains all SEs currently assigned to the delivery service.

Step 6 Check the **Primed** check box for each SE you want to prime with the live stream. For more information about priming, see the "Priming a Live Delivery Service" section on page 5-34.

Step 7 Click **Submit** to save the SE and Content Acquirer assignments.

A green circle with a check mark indicates an SE is assigned to this delivery service. To unassign the SE, click this icon, or click the **Unassign All Service Engines** icon in the task bar. Click **Submit** to save the changes.

Step 8 In the left-panel menu, choose **Live Streaming**. The Live Stream Settings page is displayed.

The Live Stream Setting page differs depending on whether you are configuring a Movie Streamer live stream or a Windows Media live stream.

Step 9 Enter the settings as appropriate. See Table 5-10 for a description of the Windows Media Live Stream Settings fields, and Table 5-11 for a description of the Movie Streamer Live Stream Settings fields.

Table 5-10 Windows Media Live Stream Settings Fields

Field	Description
Live Source URL	The URL of the origin Windows Media encoder or Windows Media server using the following format: • http://*WMencoder_or_WMStreamerServer*:*port*/*path*/*file* • rtsp://*WMencoder_or_WMStreamerServer*:*port*/*path*/*file* For encoder failover, you can specify more than one encoder. Separate live source URLs in the list by using a semicolon (;). **Note** 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.
Enable Unicast Delivery to Client	If enabled, the program uses unicast transmission.
Unicast URL Reference	If **Enable Unicast Delivery to Client** 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.
Customized URL	**Note** This is a Release 2.0 feature. This field is available when the Customized Reference URL is selected in the Unicast URL Reference field. Use one of the following formats for the custom URL for unicast: rtsp://*OriginServerFQDN/customized-name* http://*OriginServerFQDN/customized-name*
Enable Multicast Delivery to Client	If enabled, the program uses multicast transmission.
Multicast URL Reference	If **Enable Multicast Delivery to Client** 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 **Enable Multicast Delivery to Client** is checked.

Table 5-10 Windows Media Live Stream Settings Fields (continued)

Field	Description
Customized URL	**Note** This is a Release 2.0 feature. This field is available when the Customized Reference URL is selected in the Multicast URL Reference field. Use the following format for the custom URL for multicast: **http://*any SEinLiveDeliveryService/customized-name.nsc***
Multicast Address and Port	The multicast address and port to use for streaming this program using multicast. The address range is 224.0.0.0 to 239.255.255.255. The port number must be even, and within the range of 1 to 65535. These values must be unique within the system. **Note** Auto Select is a Release 2.0 feature. Click **Auto Select** to select a multicast address from the multicast address pool. See the "Configuring a Multicast Address Pool" section on page 5-38 for more information.
Multicast TTL	Specify the multicast time to live (number of hops). The default is 15 hops.

Table 5-11 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, select either **rtsp** or **http**, 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. In Release 2.2, when you click the **Auto Populate** button, the Incoming Live Streams Settings fields (the next section on the Live Streaming Settings page) are automatically populated based on the Origin Server SDP File URL **Note** In Releases 2.0 and 2.1, the Content Acquirer port must be zero (0) if the source is multicast push.
Backup SDP URL	The backup URL for the SDP file. This field is only for RTSP. Add a valid backup URL and click **Auto Populate**. The Incoming Live Streams Settings backup fields (the next section on the Live Streaming Settings page) are automatically populated based on the Backup SDP URL The Cisco CDS only supports failover between a primary Content Origin server and a backup Content Origin server for a Movie Streamer live program when the backup Content origin server uses the same codec as the primary. In Release 2.2, when you click the **Auto Populate** button, the Incoming Live Streams Settings fields (the next section on the Live Streaming Settings page) are automatically populated based on the Backup SDP File URL **Note** This is a Release 2.2 feature.
Incoming Live Streams Settings[1] **Note** Manually enter these fields when Auto Populate cannot parse the SDP URL.	
Primary Source Server	The stream source IP address.
Backup Source Server	The backup stream source IP address.
Primary 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 Acqurier 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.
Outgoing Live Streams Settings	

Table 5-11 Movie Streamer Live Stream Settings Fields (continued)

Field	Description
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.
Customized URL	**Note** This is a Release 2.0 feature. This field is available when the Customized Reference URL is selected in the Unicast URL Reference field. Use one of the following formats for the custom URL for unicast: rtsp://*ServiceRouterDomainName/program-name* http://*ServiceRouterDomainName/program-name* This URL points to a meta file (SDP) that is generated and resides on an external server.
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 **Enable Multicast Delivery to Client** check box is checked. Use the following format for the multicast URL reference (Announce URL): http://*sourceHost_or_FQDN/path/filename.sdp* This URL points to a meta file (SDP) that is generated and resides on an external server.
Multicast TTL	Specify the multicast time to live (number of hops). The default is 15 hops
Multicast Address	**Note** This is a Release 2.2 feature. 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	**Note** This is a Release 2.2 feature. The multicast port to use for streaming this program using multicast. The port number range is 1 to 65535. These values must be unique within the system.
Live Streams[2]	
Source Server	The stream source IP address. Click **Add New Live Stream** to add another live stream.

Table 5-11 Movie Streamer Live Stream Settings Fields (continued)

Field	Description
Content Acquirer Port	The port number on the Content Acquirer that will receive the stream. **Note** To activate failover support for the Content Acquirer, you must enter zero (0).
Multicast Address and Port	The multicast address and port to use for streaming this program using multicast. The address range is 224.0.0.0 to 239.255.255.255. The port number range is 1 to 65535. These values must be unique within the system. **Note** Auto Select is a Release 2.0 feature. Click **Auto Select** to select a multicast address from the Multicast Address pool. See the "Configuring a Multicast Address Pool" section on page 5-38 for more information.

1. The Incoming Live Streams Settings section is new for Release 2.2.
2. The Live Streams section is for Releases 2.0 and 2.1. You can define up to ten live streams for each Movie Streamer live program. Movie Streamer programs can have more than one live stream (audio, video, and slides).

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 **Trash** icon next to the Initial Start Time.

Step 13 Enter the settings for the playtime as appropriate. See Table 5-12 for a description of the fields.

Table 5-12 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.
Repeat Frequency	The repeat frequency has the following options: • Do Not Repeat—Plays once. • Repeat Every—Repeats every so many days, hours, or minutes. • Repeat Weekly—Repeats at the same hour on the days you choose.
Repeat Forever Repeat Until	These fields display when **Repeat Every** or **Repeat Weekly** 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 Content Origin server. Primed streams can be monitored because they are buffered on the SE.

Configuring a Rebroadcast

Once you have defined the program type, 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 5-27).

Note For rebroadcast programs, media can only be selected from one delivery service. The SEs and device groups assigned to the delivery service are selected automatically when you choose the media files for the program.

To configure a Movie Streamer rebroadcast or Windows Media rebroadcast program, do the following:

Step 1 After you have chosen a program from the Program Table page, click **Select Media**. The Select Media page is displayed.

Step 2 Choose a delivery service from the list by clicking the radio button next to the name of the delivery service and click **Show Media in Selected Delivery Service**. The Media File Selection pane is displayed.

Step 3 In the **Criteria** field, enter the search criteria for the media files you want to add to the program and click **Use Criteria**. All the media files that match the search criteria are displayed.

Use an asterisk (*) to match any number of characters, or a question mark (?) to match exactly one character. For example, use "*.mpg" for all files with the suffix "mpg," and "file?.mpg" to match file1.mpg, file2.mpg, and so on.

To start a new search, click **Select Media**.

To choose a new delivery service to choose files from, click **All Delivery Services**, choose a delivery service, and click **Show Media in Selected Delivery Service**.

Step 4 Check the **Pick** check box next to each file you want to rebroadcast and click **Add Media**. The files are displayed in the Media Files in Program pane.

To select all files, click **All**. To deselect all files, click **None**. The file list can span several pages. To see the files from the other pages, click the page number, or from the **Row** drop-down list, select one of the options.

Step 5 In the Media Files in Program pane, use the Up arrow and Down arrow next to each file to alter the order of the files. Files are played in the order in which they are listed.

Note The Up arrow and Down arrow are only displayed if the list of media files in the program is sorted by position. If you sort the media files by name or length, the arrows are not displayed.

Note Only one media file can be selected for Movie Streamer rebroadcasts.

To remove a media file from the list, check the **Pick** check box next to the file, and click **Remove Media**. To select all files, click **All**. To deselect all files, click **None**.

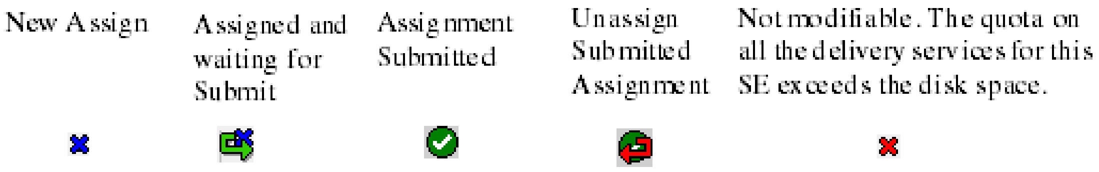
Step 6 Click **Submit** to save the settings.

Note For rebroadcast programs, media can only be selected from one delivery service. The SEs assigned to that delivery service are selected automatically when you choose the media files for the program. If at a later time you add new SEs to the delivery service, you must manually add them to the program.

Step 7 To add new SEs to the rebroadcast program, from the left-panel menu click **Assign Service Engines**. The Service Engine Assignment page is displayed.

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 5-15.

Figure 5-15 SE Assignment State


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

A green arrow wrapped around the blue X indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon.

Step 9 From the **Assign Content Acquirer** drop-down list in the task bar, choose an SE to be the Content Acquirer for this rebroadcast delivery service.

The list contains all SEs currently assigned to the delivery service.

Step 10 Check the **Primed** check box for each SE you want to prime with the rebroadcast stream. For more information about priming, see the "Priming a Live Delivery Service" section on page 5-34.

Step 11 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** in the task bar. Click **Submit** to save the changes.

Step 12 From the left-panel menu, choose **Streaming**. The Streaming Settings page is displayed.

Step 13 Enter the settings as appropriate. See Table 5-13 for a description of the Windows Media Rebroadcast Stream Settings fields, and Table 5-14 for a description of the Movie Streamer Rebroadcast Stream Settings fields.

Table 5-13 Windows Media Rebroadcast Stream Setting s Fields

Field	Description
Multicast 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 rebroadcast. 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 the Customized Reference URL is selected in the Multicast URL Reference field.
Customized URL	**Note** This is a Release 2.0 feature. This field is available when the Customized Reference URL is selected in the Multicast URL Reference field. Use the following format for the custom URL for multicast: http://*anySEinDeliveryService/program-name.nsc*
Multicast Address and Port	The multicast address and port to use for streaming this program using multicast. The address range is 224.0.0.0 to 239.255.255.255. The port number range is 1 to 65535. These values must be unique within the system. **Note** Auto Select is a Release 2.0 feature. Click **Auto Select** to select a multicast address from the multicast address pool. See the "Configuring a Multicast Address Pool" section on page 5-38 for more information.
Multicast TTL	Specify the multicast time to live (number of hops). The default is 15 hops.

Table 5-14 Movie Streamer Rebroadcast Stream Settings Fields

Field	Description
Multicast 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 rebroadcast. Choose one from the drop-down list. **Note** The Content Acquirer port must be zero (0) if the source is multicast push.
Customized URL	**Note** This is a Release 2.0 feature. This field is available when the Customized Reference URL is selected in the Multicast URL Reference field. Use one of the following formats for the custom URL for unicast: http://*sourceHost_or_FQDN/path/filename.sdp* rtsp://*ServiceRouterDomainName/program-name* http://*ServiceRouterDomainName/program-name* This URL points to a meta-file (SDP) that is generated and resides on an external server.
Multicast TTL	Specify the multicast time to live (number of hops). The default is 15 hops
Multicast Address and Port	The multicast address and port to use for streaming this program using multicast. The address range is 224.0.0.0 to 239.255.255.255. The port number range is 1 to 65535. These values must be unique within the system. **Note** Auto Select is a Release 2.0 feature. Click **Auto Select** to select a multicast address from the multicast address pool. See the "Configuring a Multicast Address Pool" section on page 5-38 for more information. **Note** 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 **Add Multicast Address/Port** to add another multicast address pool.

Step 14 Click **Submit** to save the settings.

Step 15 From the left-panel menu, choose **Schedule**. The Schedule page is displayed.

Step 16 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 **Trash** icon next to the Initial Start Time.

Step 17 Enter the settings for the playtime as appropriate. See Table 5-15 for a description of the fields.

Table 5-15 Playtime Fields

Field	Description
Start Playback on	The start date and time for the program.
UTC or SE (Local) Time	Which clock the start time should use, UTC or SE local.
Duration	The length of the program. In the drop-down list, choose minutes, hours, or days as the unit of time.
Playback Options	The playback options are the following: • Playback Once and Stop • Loop for number of minutes, hours, or days
Repeat Frequency	The repeat frequency has the following options: • Do Not Repeat—Plays once. • Repeat Every—Repeats every so many days, hours, or minutes. • Repeat Weekly—Repeats at the same hour on the days you choose.
Repeat Forever Repeat Until	These fields display when **Repeat Every** or **Repeat Weekly** 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 18 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.

Configuring a Multicast Address Pool

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 SE, 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, or you can have the CDSM select one of the addresses from the multicast address pool. Addresses are allocated for the life of a program.

When you request a specific address or a set of addresses to be used for a program, the CDSM issues only those addresses that are not used by any existing programs. If no addresses are available from the pool, or if the multicast pool has not been configured, users receive an error message.

To configure a pool of multicast addresses to be used for programs, do the following:

Step 1 Choose **Services > Live Video > Multicast Addresses**. The Multicast Addresses page is displayed.

Step 2 In the **Start Address** field, specify the first multicast IP address in the pool.

The range is 224.0.0.0 to 239.255.255.255.

Step 3 In the **End Address** field, specify the last multicast IP address in the pool.

The range is 224.0.0.0 to 239.255.255.255.

Step 4 In the **TTL field**, specify the time-to-live (number of hops) for all addresses configured in the pool.

The range is 1 to 255.

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

The list of multicast addresses that have been currently configured for specific programs is displayed in the Multicast Address table. The User Specified column displays *true* if the user has already specified the particular address for a program.

Viewing Programs

The Programs Table page lists all of the programs defined in your CDS network. Programs can be defined through the CDSM or through an API.

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 5-41 for more information.

To view all the programs defined in your CDS network, follow these steps:

Step 1 Choose **Services > Live Video > Live Programs**. The Programs Table page displays with a list of all the programs that have been defined through either the CDSM or the Program API.

Step 2 Click the **Day**, **Week**, **Month**, or **Year** tab to view the playback schedules. Scheduled programs are listed by start time (initial start time plus any repeat intervals). Times begin with the current device time (current system time plus device time zone offset).

The **Unscheduled** tab displays all unscheduled programs defined in your CDS network. The **All** tab displays all the programs defined in your CDS 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 5-16 describes the information that is displayed in this page.

Table 5-16 Programs Table Page Information

Item	Description
Tabs	
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 5-16 Programs Table Page Information (continued)

Item	Description
Program Listing Table	
Program	Program name, which must be unique to the CDSM.
Type	Program type. Program types are: • Movie Streamer live • Movie Streamer rebroadcast • Windows Media live • Windows Media rebroadcast
Schedule	Describes the schedule. Options are: • None (the program has no schedule) • Loop continuously • Number of playtimes (the number of times that the program is scheduled to be shown) 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 reparsing it. The program file supports RTSP.

In contrast, programs defined using the CDSM are not based on a program file; instead, the settings entered in the CDSM are saved directly to the database.

Programs created using an API can be viewed in the CDSM as read-only, and modifications to API programs can be done through the API. You can also edit the API program using the CDSM; however, if you choose this option, the information about the API program file is deleted and the program can no longer be modified through the API. A third option is to copy the API program using the CDSM Copy Program feature. The new copy will not contain the program file information and will be treated as a CDSM-generated program for the purposes of editing. (See the "Copying a Program" section on page 5-41.)

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 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 5-27.)

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.