Cisco VDS Optimization Engine Software Installation and Configuration Guide

Release 1.0
May 2013

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

Text Part Number: OL-25945-01

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

Cisco Content Adaptation Engine Software Installation and Configuration Guide

CONTENTS

Preface

This preface describes the audience, use, and organization of the *Cisco VDS Optimization Engine Software Installation and Configuration Guide*. The preface also outlines the document conventions and support information.

This preface contains the following sections:

Document Revision History

The Document Revision History table below records technical changes to this document.

Document Version	Date	Notes
OL-25945-01	May 2013	Initial release.

Audience

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

Objective

This guide provides the information you need to install, configure, and monitor the VDS-OE. This guide also provides procedures for using the commands that have been created for use with VDS-OE features. For detailed information related to installation and infrastructure configuration, see the "Related Publications" section on page xi.

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

Document Organization

This document contains the following chapters and appendices:

Chapter or Appendix	Description
Chapter 1, "Product Overview"	Provides a brief introduction to the VDS-OE. Describes VDS-OE topology and workflow elements, and presents sample video workflows.
Chapter 2, "Installing the VDS-OE"	Describes VDS-OE deployment options, hardware requirements, and procedures for installing VDS-OE components.
Chapter 3, "Configuring the VDS-OE"	Provides an overview of VDS-OE configuration and describes configuration tasks performed from the Content Delivery System Manager (CDSM) GUI, including configuration for redundancy.
Chapter 4, "Managing and Monitoring the VDS-OE"	Describes procedures for reviewing video job records, monitoring MIBs and alarms, and managing VDS-OE processes for high availability.
Chapter 5, "Troubleshooting the VDS-OE"	Explains possible VDS-OE failure modes and describes their accompanying symptoms with regard to Offline Asset Manager (OFAM), Web Engine, and Encode Node failure.
Appendix A, "Sample Configurations"	Provides a reference configuration for the Service Engine (SE) and OFAM components of the VDS-OE.
Appendix B, "CLI Commands"	Provides information on configuring port channels, last resort routing domains, and other CLI commands.

Document Conventions

This guide uses the following conventions for command syntax descriptions and textual emphasis:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.

Convention	Description
{*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.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`italic screen` font	Arguments for which you supply values are in *`italic screen`* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets in contexts where italics are not available.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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

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

Tip Means the following information might help you solve a problem.

Related Publications

These documents provide complete information about the VDS-OE and are available from the Cisco.com site:

- Release Notes for Cisco Video Distribution Suite Optimization Engine 1.0
- Release Notes for Cisco Internet Streamer CDS 2.6
- Cisco Internet Streamer CDS 2.6 Quick Start Guide
- Cisco Internet Streamer CDS 2.6 API Guide
- Cisco Internet Streamer CDS 2.6 Command Reference
- Cisco Internet Streamer CDS 2.6 Alarms and Error Message Guide
- Cisco Internet Streamer CDS 2.6 Software Upgrade Guide
- Cisco Content Delivery Engine 205/220/250/420/460 Hardware Installation Guide

- Cisco UCS C220 Installation and Service Guide
- Cisco Content Delivery System 2.x Documentation Roadmap
- Regulatory Compliance and Safety Information for the Cisco Content Delivery Engines
- Cisco Transcode Manager Installation Guide v5.0
- Cisco Transcode Manager Quick Start Guide v5.0

You can access the software documents at the following URL:

- http://www.cisco.com/en/US/products/ps7127/tsd_products_support_series_home.html

You can access the hardware documents at the following URL:

- http://www.cisco.com/en/US/partner/products/ps10493/index.html for C-series
- http://www.cisco.com/en/US/partner/products/ps10280/index.html for B-series

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Product Overview

Overview

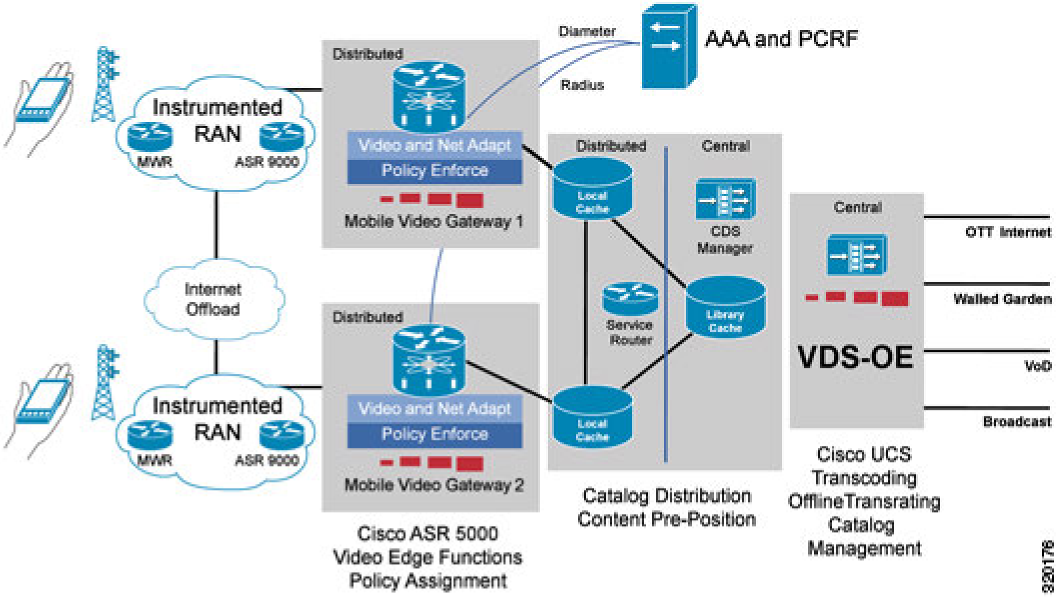
The Cisco Video Distribution Suite Optimization Engine (VDS-OE, or simply OE) is software that optimizes the delivery of managed and unmanaged video content over service provider IP networks. Using the OE to optimize video delivery reduces the impact of video content on network resources, and helps service providers maximize quality of service while minimizing cost as their networks grow.

The benefits of using the OE are made visible to service providers through statistical reporting tools in the Content Delivery System Manager (CDSM), a separate Cisco application that shows the effects of OE operation on network efficiency and loading. The tools in CDSM can also help service providers calibrate the OE for best effect and determine the most cost-effective strategies for network growth.

The OE forms part of the Cisco Video Distribution Suite (VDS), which has these core components:

- The Cisco Mobile Video Gateway (MVG), dedicated software running on a Cisco ASR 5000 Series Multimedia Core Platform. The MVG uses deep packet inspection (DPI) to analyze video traffic and determine the steering, formatting, and pacing of each content stream.
- The OE, dedicated software running on a Cisco Unified Computing System (UCS) infrastructure. The OE optimizes the delivery of OTT video content based on the requesting device, the popularity of the video, and current resource loading, and also provides video catalog management services.
- The Cisco Transcode Manager (CTM), an integral component of the OE that provides online and offline video transcoding services. In this document, the CTM is also referred to as the Transcoder.

Figure 1-1 Cisco Mobile Videoscape Solution



Note Service providers who do not opt for a complete Cisco mobile video solution can still use the OE in conjunction with an existing DPI gateway and content delivery system. The OE provides enough functionality on its own to be used in standalone or third-party deployments.

Operation

The OE supports both progressive download and Adaptive Bit Rate (ABR) streaming in HTTP Live Streaming (HLS) format. Simply described, the OE performs the following functions:

- Receives customer requests for video content.
- Decides whether and how that content can be optimized.
- Submits video optimization jobs to the Transcoder as needed.
- Streams the optimized video for delivery to the requester.
- Caches popular optimized video in network storage or a local cache

In deciding whether and how to optimize video content, the OE takes the following factors into account:

- Capabilities of the requesting playback device.
- Current popularity of the requested video.
- Whether the video is already cached, and in what form.
- Original video quality, expressed in bit rate and frame rate.
- Gains (if any) expected from transforming the video content.
- Profile (e.g., billing plan) of the end user.
- Whether the content provider is a partner of the service provider.
- The resolution of the original video

- Whether transcoding is to be performed online or offline

After analyzing the factors involved in the decision to optimize, the OE performs one of the following tasks:

- Serves video with online transcoding.
- Serves video from cache in the best format and data rate for the playback device.
- Ingests the video, make one or more cached copies, and then serve the video.
- Allows the video to pass unmodified from the origin server to the user equipment.

The OE can be configured to serve both over-the-top (OTT) content and managed domain content. Both OTT and managed domain content can be transcoded either online or offline.

Note Contact your Cisco representative for details on using the OE in Mobile Videoscape deployments.

OE Components

The OE consists of individual software and hardware components that work together to manage video delivery. The OE includes the following major components:

- Service Engine (SE), the processing component of the OE that performs the actual video serving function; also known as the Web Engine
- Storage for transcoded video files
- Offline Asset Manager (OFAM), the component of the OE that maintains a database of video assets and manages the creation and deletion of stored or cached video
- Cisco Transcode Manager (CTM), also known as the Transcoder, an application integral to the OE that transcodes media for offline or online optimization
- CDSM, a separate application that is used to manage the OE through a graphical interface
- Service Router (SR), an optional component used only with managed domain services

When installed and configured on a UCS server platform, these components create a single logical entity that is referred to collectively as the OE. Human operators communicate with all components of the OE through the CDSM Web browser GUI.

Note The OE can be configured for split mode operation. In split mode, the SE and OFAM can run on separate nodes.

OE Functions

As a system, the OE supports the following functions:

- Online and offline progressive video transcoding
- Offline ABR video transcoding and manifest file modification
- Access control list (Blacklist/Whitelist)
- Non-video data bypass
- Service Engine load balancing

- Global popularity tracking of media
- Centralized and localized caching
- Media policy control and enforcement
- Media acquisition from the NAS
- Source IP address ranging and proxy
- Progressive and ABR media serving
- Transaction log generation

This section highlights some of these features and related concepts.

Tip A general understanding of these features and concepts is helpful in completing the installation, configuration, and management tasks detailed later in this guide.

Online and Offline Progressive Video Transcoding

The OE calls the Transcoder as needed to transcode media prior to delivery. The OE uses transcoding to modify the bit rate, resolution, frame rate, and other parameters to compress video while maintaining quality.

The OE applies transcoding profiles for the video codec and device before serving the video to the subscriber via the MVG. The following table lists the source and target formats supported by the OE for both offline and online transcoding.

Table 1-1 CAE Supported Transcoding Combinations

Input Parameters	Output Parameters
Video: H.264 Audio: AAC Container: MP4	Video: H.264 Audio: AAC Container: MP4
Video: H.264 Audio: AAC Container: FLV	Video: H.264 Audio: AAC Container: FLV

Offline ABR Video Transcoding and Manifest File Manipulation

ABR video optimization is achieved through modification of the manifest file. The manifest file is modified to present an optimum selection of bit rates to the user equipment (client). Manifest file manipulation may involve inserting new ABR rates or deleting existing ones, or both. For example, a higher rate can be remove and a lower rate added.

Service Engine Load Balancing

For each video request received, the MVG assesses the load on each SE in the domain; selects a SE on that basis to service the request; and then readdresses the request to the selected SE. The MVG maintains a list of the IP addresses for each SE in its virtual server group.

Global Popularity Tracking of Media

While serving video to subscribers, the OE tracks the popularity of the video based on the number of requests received for that asset in a given time period. When a particular video asset reaches a popularity threshold, the OFAM that manages the asset performs offline transcoding of the asset. When multiple OFAMs are deployed in the network, the popularity counters collected by each individual OFAM are aggregated into a master database on the CDSM node.

Centralized and Localized Caching

If a particular video meets a popularity threshold through repeated requests, the OE acquires the video from the original website, transcodes it, and saves it to a centralized NAS. When the SE serves the video for the first time, it acquires the video from the NAS and saves it to its local cache. For any subsequent video requests, the SE acquires the video from its local cache.

If the requested video is not in cache but meets a predefined popularity threshold, the SE not only orders real-time (online) transcoding of the video received from the origin server, but also triggers the OFAM to perform offline transcoding to create one or more cached copies of the video.

Media Policy Control and Enforcement

Media policy control and enforcement determines how video assets are transcoded and served, based on the following criteria:

- Adaptation Profile Index, based on subscriber service level
- Device Class, based on device capabilities
- Source content, identified by matching domain name
- Input video bit rate
- Input video frame rate
- Input video resolution
- Container format
- Video codec employed
- Whether transcoding is to be online or offline
- Whether the content provider is a partner of the service provider
- Whether the request falls into the configured blacklist or whitelist

Support for Radio Access Technology (RAT)

Different types of radio access technology (RAT) or access networks can support different network bandwidths. This makes it necessary for the OE to use the access network type as one criterion when performing content adaptation. To support RAT, the MVG should be able to idenfity the RAT type on a per-subscription or per-session basis and send that information to the OE in the form of an X-header for related HTTP GET requests.

Support for 3GP and 3G2 Video

VDS-OE allows 3GP and 3G2 video content (3GPP and 3GPP2 file formats) to be tracked for popularity and, after reaching a predefined threshold, cached in NAS or local storage for offline serving. Because 3GP and 3G2 video is already of low quality, VDS-OE does not attempt to further optimize the video, as this would usually lead to video of unacceptable quality. Even so, local caching allows for bandwidth savings in the core network.

Media Acquisition from the NAS

The OE NAS stores both transcoded video files and ABR manifest files. These files are not removed by the SE. Instead, the OFAM deletes files from NAS in accordance with the following deletion criteria:

- The OFAM keeps an expiration timer for transcoded video, and deletes files after they expire.
- The OFAM employs a NAS eviction mechanism that works to prevent the storage capacity of the NAS from falling below a configured "high watermark" threshold (75% by default). This ensures that there is always room in the NAS for new input or output files.
- The OFAM database includes entries for last access time that can serve as triggers for eviction of files that have not been used recently. The OFAM also periodically checks for and deletes any "dangling" files, which are files that no longer have a database entry.

Note While the SE cannot delete expired content from the NAS, the content cached in local storage is deleted automatically when the hit count (number of times the content is accessed) reaches a predefined storage threshold.

Source IP Address Ranging and Proxy

As a security measure, some websites may deny service to a source that makes a large number of requests from the same IP address. To avoid this potential issue, the OE can be configured to perform IP address ranging, in which it selects one of up to 24 different IP addresses for use by the SE when making requests to a website.

Progressive and ABR Media Serving

The OE transcodes and serves both progressive and ABR video based on media policy and popularity settings. Progressive video is transcoded and served online until popularity thresholds are met; once met, the video is transcoded, cached, and served offline.

For ABR video, video chunks of different bit rates are added or deleted from original video and cached for serving after the popularity threshold has been reached. The manifest file is modified to remove or add video bit rates. New video rates are generated through transcoding.

Master Database Failover and Backup/Restore

The OE can scale to include multiple OFAMs. This is accomplished by maintaining a centralized master database to which all OFAM local databases are synchronized. By default, the master database server runs on the CDSM nodes.

Such a centralized database serves two purposes:

- Aggregates the hit count across multiple OFAMs so that offline transcoding is triggered in a predictable way.
- Allows content that was offline-transcoded by one OFAM to be served by another OFAM.

By default, the OFAM always connects to the master database on the primary CDSM. After a manual switchover of CDSMs, the OFAM should connect to the master database on the new primary CDSM.

The OFAM is designed to use multiple connections to connect to the master database for transaction throughput. The OFAM generates an alarm if its connection to the master is lost, and then clears the alarm when the connection is restored.

Managed Domain Services

VDS-OE supports optimization of both managed and OTT content. Managed content domains must be configured on the CDSM as delivery services. Each delivery service must have an associated content origin from which to retrieve video content.

VDS-OE does not support a content delivery network (CDN) or similar hierarchy. Instead, the SE receiving the request matches on a delivery service and acquires content directly from the corresponding content origin. For additional information, see Chapter 5 of the *CDS-IS 2.6 User Guide*.

The CDS-IS service router (SR) can be used to provide load balancing for managed domains. For additional information on the SR, refer to the Content Delivery System overview in Chapter 1 of the *CDS-IS 2.6 User Guide*.

Managed Domain Services Workflow

The basic sequence of events for managed domain content retrieval are as follows:

1. A client requests a video associated with a managed domain; for example, http://service.mydomain.com/video.mp4. The DNS resolves this to the SR associated with the mydomain.com delivery service.
2. The request to the SR is routed through the MVG. Although the MVG identifies it as video content, it also identifies it as a managed domain and so does not readdress the request. Instead, it is routed to the SR as normal.
3. The SR performs a 302 redirect to the URL http://service.mydomain.com/video.mp4. Once again, the request is routed through the MVG and, as before, is routed straight through to the SE.
4. On the OE, the domain name portion (mydomain.com) is extracted and used to look up the delivery service for the corresponding origin domain name. The SE substitutes the origin domain name into the URL and continues with normal SE flow for OTT content. If no domain server is found, the request proceeds as with normal OTT content, but without the mapping.

A variation of this sequence occurs when the SR is configured as an Authoritative DNS server. In this case:

1. A client requests a video associated with a managed domain; for example, http://service.mydomain.com/video.mp4. The SR Authoritative DNS eventually gets the request and resolves the request directly to one of the SEs.

2. The client gets the resolved address and issues a request of http://SE1.SE.service.mydomain.com/video.mp4. Once again, the request is routed through the MVG and, as before, is routed straight through to the SE.
3. On the OE, the domain name portion (mydomain.com) is extracted and used to look up the delivery service for the corresponding origin domain name. The SE (Web Engine) substitutes the origin domain name into the URL and continues with normal SE flow for OTT content. If no domain server is found, the request proceeds as with normal OTT content, but without the mapping.

Transaction Log Generation

For each video served, a Transaction Log is generated and stored in the OE file system. Both Extended Squid and Apache CLF formats are supported. Transaction Logs can be reviewed using the web application AnalysisUtility tool, and can be archived and uploaded to an external FTP server. For more information, refer to the *CDS-IS 2.6 Sofware Configuration Guide*.

Sample OE Workflows

The following sample workflows show how video content is served in a variety of representative use cases.

Request for Cached Progressive Video

In this scenario, we assume that a user device has requested a progressive video file that has already been transcoded and cached by the OE through a previous offline transcoding session. The following events take place:

1. A user device sends an HTTP GET request for the video.
2. The MVG receives the user request and, using DPI, determines that it is a request for video. The MVG then refers to its OE load-balancing scheme to select an active SE, and forwards the HTTP request to the selected SE.
3. The SE receives the request from the MVG and verifies through the OFAM that a video meeting the necessary device and policy requirements is cached. If a suitable video is cached, the SE retrieves the video from the location specified by the OFAM and sends it to the MVG.
4. The MVG receives the video from the SE and forwards the video to the user device.

Video Served from the NAS and Saved to Local Cache

When the OE receives a request for a popular video, it acquires the video from the original website, transcodes it, and saves it to the NAS. When the SE serves the video for the first time, it acquires the video from the NAS and saves it to its local cache. For any subsequent video requests, the SE acquires the video from its local cache.

Request for Uncached Progressive Video

In this scenario, we assume that a video is requested that is not available either in the NAS or in the local cache, and so must be served from the original website with online (real-time) transcoding applied. The following events take place:

1. A user device sends an HTTP GET request for the video.

2. The MVG receives the user request and, using DPI, determines that it is a request for video. The MVG then refers to its OE load-balancing scheme to select an active SE, and forwards the HTTP request to the selected SE.
3. The SE receives the HTTP request from the MVG and determines through the OFAM that the requested video is not cached. The OFAM also finds that the requested video does not meet the predefined popularity threshold, and so does not initiate offline transcoding of the video.
4. The SE receives the video from the origin server and submits it to the Transcoder with a request to perform online (real-time) transcoding of the video in a specific format and bit rate.
5. The Transcoder transcodes the video in the specified format and bit rate and returns the transcoded video data to the SE, which in turn sends the transcoded video data to the MVG.
6. The MVG receives the video from the SE and forwards the video to the user device.

Request for Progressive Video Not in Cache, but Popular

If the requested video is not in cache but meets a predefined popularity threshold, the OE orders online transcoding of the video it receives from the origin server, and also orders offline transcoding to create one or more cached copies of the video. In this case, the workflow is as described above, but with an additional process that proceeds in parallel as follows:

1. The OFAM determines that the video is popular, downloads the video from the origin server, and submits a video transcosing request to the Transcoder to perform offline transcoding of the video in a specified format and bit rate.
2. The Transcoder selects an encode node based on its own configuration and load-balancing mechanism, transcodes the video as requested, and saves the output files to the specified NAS directory.
3. The OE receives a notification from the Transcoder that the transcode job is finished, and in response, updates the state of the database record for the transcoded video asset to READY.

Request for Cached ABR (HLS) Video

In this scenario, we assume that an ABR video is requested that is already cached in the OE. The following events take place:

1. The user device sends an HTTP GET request for an HLS playlist corresponding to the ABR video.
2. The MVG receives the user request and, using DPI, determines that this is a request for video. It then refers to its OE load-balancing scheme to select an active SE, adds information relevant to the ABR video to the HTTP request, and forwards the HTTP request to the selected SE.
3. The SE receives the HTTP request from the MVG and determines through the OFAM that the requested playlist is cached, and requests the playlist from the local cache or NAS.
4. The SE receives the playlist, which has been modified by the CAE, from the OFAM and forwards it to the MVG. The MVG, in turn, forwards the OE-modified playlist to the user device.
5. The user device returns repeated HTTP requests to the MVG for the ABR segments required to play the entire video. The MVG, in turn, sends repeated requests to the SE, which provides the ABR segments as they are requested.

ABR (HLS) Video Not in Cache, but Popular

The OE currently does not support online (real time) transcoding of ABR video. Therefore, if a requested ABR video is determined to meet a predefined popularity threshold, the OE retrieves the video content directly from the origin server.

Installing the VDS-OE

Overview

This chapter describes system requirements and design considerations for the OE and provides instructions for installing the OE and related software.

Hardware Platform

The OE and its required CDSM management system run on the Cisco UCS hardware platform. The installation is implemented on the 1RU Cisco UCS C-series chassis. A typical OE hardware configuration includes the following:

- Cisco UCS C-series with:
  - Hyperthreading enabled
  - Two 10 Gigabit unified fabric
  - Eight (8) hard disks in RAID5 configuration
  - 48 GB DDR3 memory
- UCS blade servers for CTM
- NAS

This platform can be used as the hosting environment for the CDSM, OFAM, and SE together, or for the SE alone with CDSM and OFAM installed on a different server. These two options benefit from slightly different hardware configurations. The SE alone requires substantial local storage for caching video content. The maximum local storage currently provided on UCS C-Series blades is about 1.2 TB. Typically, the SE is implemented on a C220 M3 with eight 300 GB hard disks.

Tip Consult Cisco UCS product information for current disk and configuration settings.

Although 48 GB DDR3 memory is the nominal recommended configuration, the C220 M3 supports up to 384 GB of memory, so much more can be added if desired. Additional memory allows more streaming content to remain in memory, thereby optimizing transcoding node utilization and thus yielding higher overall performance.

Like the SE and CDSM, the CTM is typically installed on a UCS blade server. A typical installation may have 10 or more transcoder blades for every OFAM or SE installed. Ideally, the transcoders are installed in a UCS chassis and are managed collectively by UCS Manager. Otherwise, the transcoders can also run independently on individual C Series chassis.

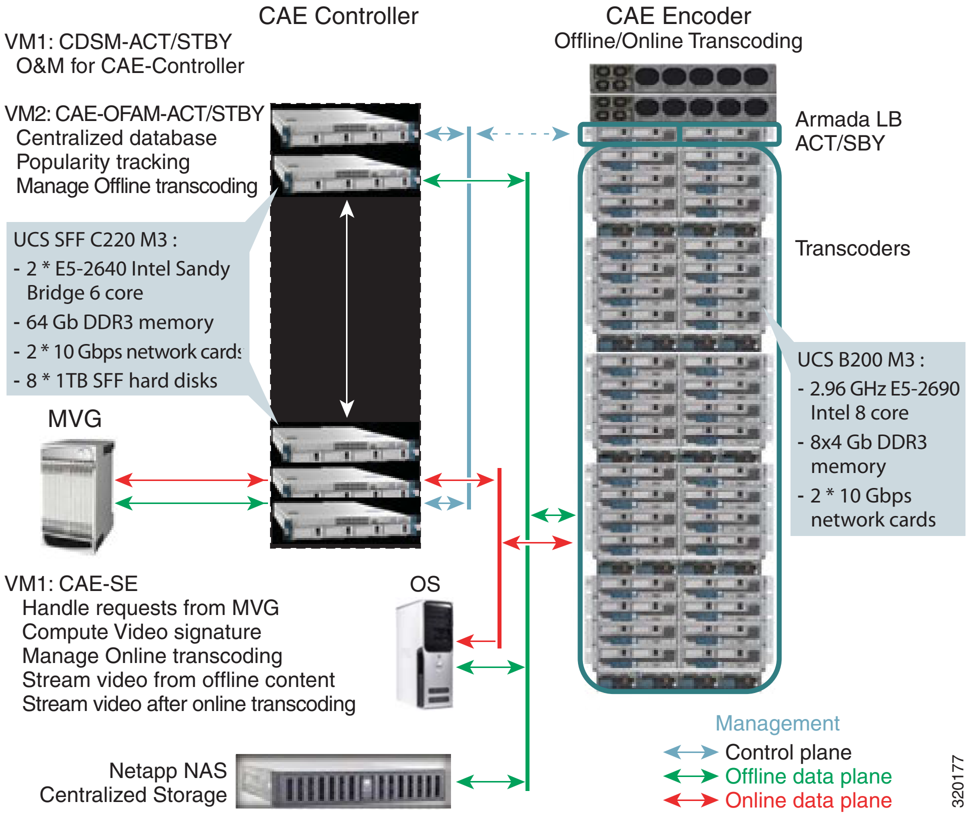
Transcoded video is saved either to the NAS or to the OE local disk. Total space requirement for video can be estimated as follows:

- Space required = number of videos * average video rate * average duration

For example, a 15-TB storage array can hold 100,000 six-minute videos encoded at 500 Kb/s average.

Figure 2-1 shows the basic configuration for CDSM, OFAM, SE, and CTM hardware.

Figure 2-1 CAE Solution Components



Requirements for Redundancy

The CDSM and the OFAM support redundancy. A redundant CDSM and OFAM can be added by installing another UCS C-series blade server.

OFAM Redundancy

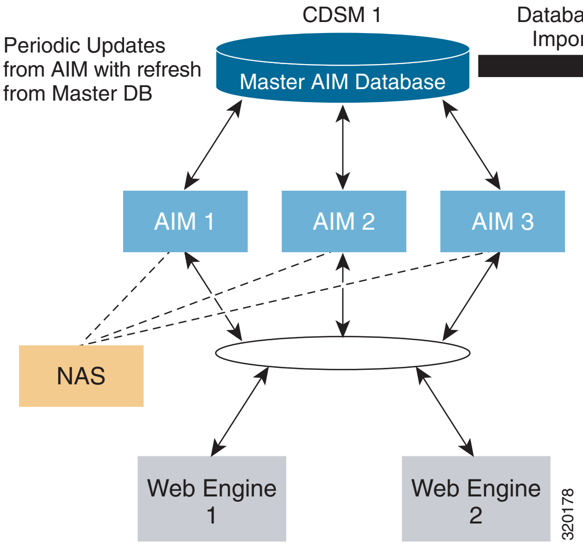
Video asset information is maintained in the Asset Information Manager (AIM) within the OFAM. Scalability and redundancy are acheived through multiple AIMs, with synchronization maintained through the Master AIM Database contained in CDSM. A backup copy of the Master Database is kept in the standby CDSM. Refer to the *Cisco Content Delivery Engine 205/220/250/420/460 Hardware Installation Guide* for additional information on redundancy.

CDSM Redundancy

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

Figure 2-2 gives a graphical summary of the redundancy architecture for CDSM.

Figure 2-2 CDSM Redundancy Architecture



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 CDSM design principle is that the management device is never in the service delivery path. When the CDSM fails, the rest of the CDS 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 CDS. As soon as a failure to connect to the CDSM is noticed, the administartor can activate the standby CDSM.

AIM Redundancy

Each Web Engine (CAE-SE) is configured to connect to one primary or secondary AIM (CAE-OFAM). If the Web Engine’s connection to the primary fails, it will automatically switch its connection to the secondary AIM. Furthermore, if the connection to the secondary AIM is lost, the Web Engine will switch its connection to the primary AIM.

Operating System Requirements

The OE system requires VMware ESXi-5 hypervisor. The SE, OFAM, and CDSM components of the OE each run in a separate VMware virtual machine (VM). VMware is installed directly on the UCS server, and a single image is used for all CDSM and OE servers. The processes that each server supports and launches are set using a configuration file.

Installation of the OE also requires installation of CTM. The CTM encode servers run under Windows and are managed and monitored separately by the CTM Manager GUI.

See the following documents for CTM installation requirements and procedures.

- *Cisco Transcode Manager Installation Guide v5.0*
- *Cisco Transcode Manager Quick Start Guide v5.0*

Installation Procedures

Installation of the OE and its related components involves the following procedures:

1. Install the UCS Server
2. Install and Configure VMware
3. Install and configure the SE, OFAM, and CDSM Image

This section describes each of these procedures in detail.

Installing the UCS Server

For instructions on UCS blade server installation, refer to the *Cisco UCS C220 Installation and Service Guide*. This document is available in PDF format at no cost from www.cisco.com. If you encounter issues not covered in the manual, contact your Cisco representative for assistance.

Repurposing an Existing Server

To reuse an existing server, you may first need to reconfigure the storage and memory resident on the server to meet the requirements of OE and related software. Refer to the server instructions for the appropriate procedures.

Installing and Configuring VMware

Install VMware ESXi5 hypervisor and configure it for the number of VMs required to run all OE components hosted on the server (SE, OFAM, CDSM).

Hardware Configuration for VMs

The VM for the SE component should run on its own server. We recomend that you run the VMs for CDSM and OFAM on the same server hardware, equipped as follows:

- At least two 10G ports
- 8 x 300 GB hard disks in RAID5 configuration

- At least 48 GB DDR3 memory
- Hyperthreading enabled

Installing VMs on Cisco Servers

Detailed instructions for installing VMware on Cisco C-Series servers is provided in the *Cisco UCS C-Series Servers VMware Installation Guide*.

This document is available in PDF format at no cost from www.cisco.com. The sections most relevant for OE installation are "VMware vSphere ESXi Installation" and "RAID Controller Considerations." These sections may be downloaded separately from the following URLs:

- http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/CSERIES-VMWARE_chapter_011.pdf
- http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/CSERIES-VMWARE_appendix_0101.pdf

Note Be sure to select RAID-5 when setting up the hard disks for the server. This means that, for the UCS C220M3 with eight hard disks, these hard disks will be presented as one virtual disk.

Configuring Ports as Pass-Through Devices

For optimum performance, the 10G ports on the SE servers must be configured as pass-through devices. To configure these ports, do the following:

Step 1 Launch the **VMware vSphere Client** application.

Step 2 From the **Inventory** listing, choose the **ESX host** that is to be configured.

Step 3 In the Configuration tab, click **Advanced Settings**. The **Pass-through Configuration** page is displayed, listing the available pass-through devices (ports).

Step 4 Click **Edit**, then select the devices to be configured.

Step 5 Click **OK**, and confirm that the icon by each device selected has changed from green to orange, indicating changed status.

Step 6 Reboot the server, return to the **Pass-through Configuration** page, and confirm that the icons for all devices selected has changed from orange to green, indicating enabled and active status.

Installing VM Components

The SE, OFAM, and CDSM components of OE install in separate VMs. The OE installation includes two Open Virtual Appliance (OVA) files, one for the SE and one for OFAM and CDSM:

- VDSOE_SE.ova
- VDSOE_OFAM_CDSM.ova

Each OVA file installs on the VMware ESXi host on the Cisco UCS server using the VMware vSphere client software.

Default VM settings in the OVA file are as follows:

- 5 disks

- 16 GB memory
- 2 NICs:
  - For SE: should be mapped to the two 1 Gig interfaces for management and control. The 10G ports will be added for the datapath as passthrough in the description below.
  - For OFAM: should be mapped to the two 10 Gig interfaces for management and control
- CPU: 12 cores

Complete the following steps to install the VM components:

Step 1 Log into the **VMware vSphere Client** application.

Step 2 Choose **Home > Inventory > Hosts and Clusters**.

Step 3 Select the **host** that is to receive the installation.

Step 4 Choose **File > Deploy OVF Template**.

Step 5 Enter the **URL** or **disk** where the OVA file (which contains the OVA template) is located.

Step 6 Follow the prompts to install the OVA file.

Step 7 Confirm that the network interfaces are mapped correctly between the OVA template and the new VM being instantiated.

Step 8 In the case of the SE, configure the 10G ports in passthrough mode on VMware as described in VMware Knowledge Base document 1010789, “Configuring VMDirectPath I/O pass-through devices on an ESX/ESXi host,” available from the VMware website.

a. Return to the **Inventory** page, right-click the **VM**, and choose **Edit Settings**.

b. Click the **Hardware** tab.

c. Click **Add** and then choose the **PCI device**. (The 10G ports are located on PCI cards.)

d. Click **Next**, then repeat these steps as needed for each 10G port.

Step 9 Choose **Configuration > Networking**.

Step 10 Confirm that the following “Networks” are present:

- Management network - for CDSM, ssh, etc. connectivity (1G interface)
- Internal Control network - for control traffic between SE, OFAM, and CDSM (1G interface)
- CTM network - connects to Cisco Transcode Manager (10G interface)
- OS network (also called primary interface) - connects to the Internet (10G interface)
- Client network (also called streaming interface) - connects to the ASR5000 (10G interface)

Step 11 Repeat the steps above for the remaining OVA file.

Installing and Configuring the SE, OFAM, and CDSM Image

After the VMs are deployed and powered up, the SE, OFAM, and CDSM will boot up with default images and default configurations.

Configuring the SE

Step 1 Configure the following interfaces:

- Management network
- Internal Control Network
- Client network (Streaming interface)
- Origin Server Network (Primary Interface)
- CTM Network
  - `Interface TenGigabitEthernet x/0`
  - `Ip address <ip address> <mask>`
  - `Exit`

Step 2 Configure the default gateway:

- `ip default-gateway <ip address>`

Step 3 Configure the DNS server:

- `ip name-server <ip address>`

Step 4 Configure the primary and streaming interfaces:

- `Primary-interface <interface>`
- `Streaming-interface <interface>`

Step 5 Save the configuration:

- `Write memory`

Step 6 Reload.

Step 7 Configure the CDSM IP address:

- `cdsm ip <cdsm ip address or hostname>`

Step 8 Enable the CMS process:

- `cms enable`

Step 9 Save the configuration:

- `Write memory`

Step 10 Configure SE features from the CDSM as needed.

Configuring the OFAM

Step 1 Configure the following Interfaces:

- `Management network`
- `Internal Control network`

Step 2 Configure the default gateway:

- `ip default-gateway <ip address>`

Step 3 Configure the DNS server:

- `ip name-server <ip address>`

Step 4 Configure the primary interfaces:

- `Primary-interface <interface>`

Step 5 Save the configuration:

- `Write memory`

Step 6 Reload.

Step 7 Configure the CDSM IP address:

- `cdsm ip <cdsm ip address or hostname>`

Step 8 Enable the CMS process:

- `cms enable`

Step 9 Enable OFAM mode to start up OFAM services:

- `cae ofam-mode enable`

Step 10 Save the configuration:

- `write memory`

Step 11 Configure the OFAM features from CDSM as needed.

Configuring the CDSM

CDSM is the management system for OE. CDSM runs on a separate VM; we recommend installing it on the same UCS server as the OFAM and its VM.

Step 1 Configure the following Interfaces:

- `Management network`
- `Internal Control network`

Step 2 Configure the default gateway:

- `ip default-gateway <ip address>`

Step 3 Configure the DNS server:

- `ip name-server <ip address>`

Step 4 Configure the primary interfaces:

- `primary-interface <interface>`

Step 5 Change the device mode:

- `device mode content-delivery-system-manager`

Step 6 Save the configuration:

- `write memory`

Step 7 Reload.

Step 8 Enable the CMS process:

- `cms enable`

Step 9 Save the configuration:

- `write memory`

Configuring the VDS-OE

Overview

You must configure the OE before using it for video content delivery. This chapter explains how to perform OE configuration using CDSM.

The goals of OE configuration are:

- To establish correct operating parameters for the OE hardware
- To define the IP interfaces through which the OE interacts with the network
- To configure basic operating parameters for video transcoding and delivery

The OE allows operators to use both CDSM GUI and CLI command interfaces. Where both GUI and CLI methods exist, they are equivalent and synchronized. In fact, CDSM GUI operation is implemented by remotely executing the corresponding CLI command on a particular OE node. When using the OE together with VDS-IS, we recommend using the CDSM GUI where possible, as this allows the two applications to share a common control interface.

Tip This chapter describes procedures using the CDSM GUI. For information on using CLI commands in CDSM, see the CLI Commands appendix.

Note The CDSM supports two types of configurations, global and device. With both types of configurations, commands are downloaded from the CDSM to the device. With global configuration, commands are synchronized to the CDSM when changed on the device.

Using the CDSM

This section provides a brief overview of using the CDSM GUI. For additional information, see the relevant portions of the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide (OL-23609-01)*.

Logging In to the CDSM

To log into the CDSM, do the following:

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

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

```
https://192.168.0.236:8443
```

The Security Alert message is displayed.

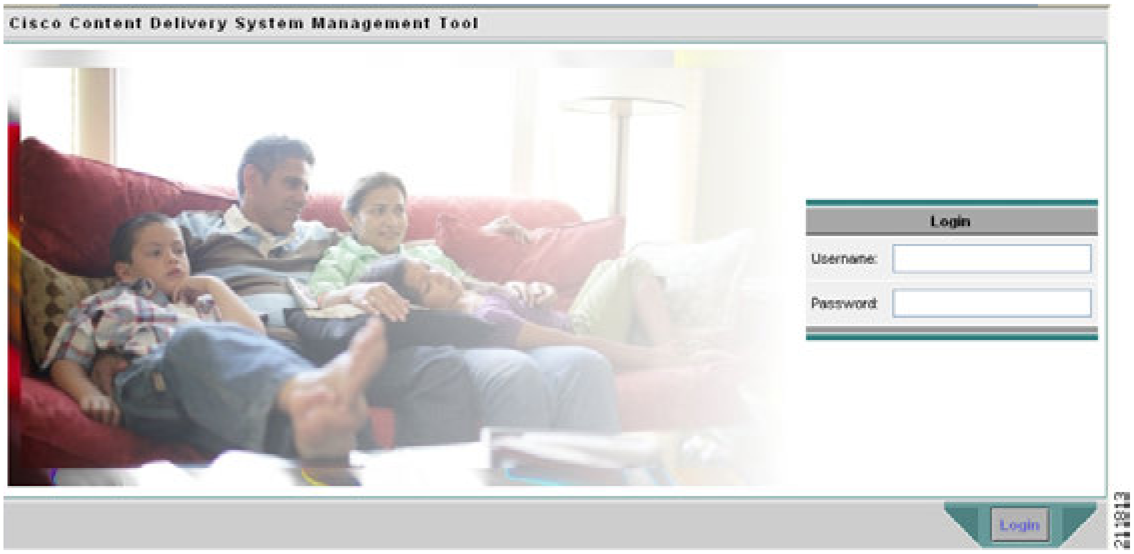
Note Sometimes the CDSM is not initially accessible from a web browser. If this occurs, you must disable and re-enable the Centralized Management System (CMS), log in to the CLI for the CDSM, and enter the global configuration command **no cms enable** followed by **cms enable**. You must ensure that the CMS is enabled in order to access the CDSM GUI.

Note Do not try to access a single CDSM through two or more different web browser windows. The actions you take in one window will not always affect the results shown in other windows.

Note If you are using Mozilla Firefox version 3.01 or higher 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 has been added to the exception list and you no longer get the Secure Connection Failed message.

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

Figure 3-1 CDSM Login Page



Step 3 Enter the **Username** and **Password**, then click **Login**. The CDSM home page is displayed.

Note When logging into the CDSM for the first time, do not set your browser to remember your CDSM username and password. Doing so would cause the browser to remember the default admin username and password, which you should change as soon as possible.

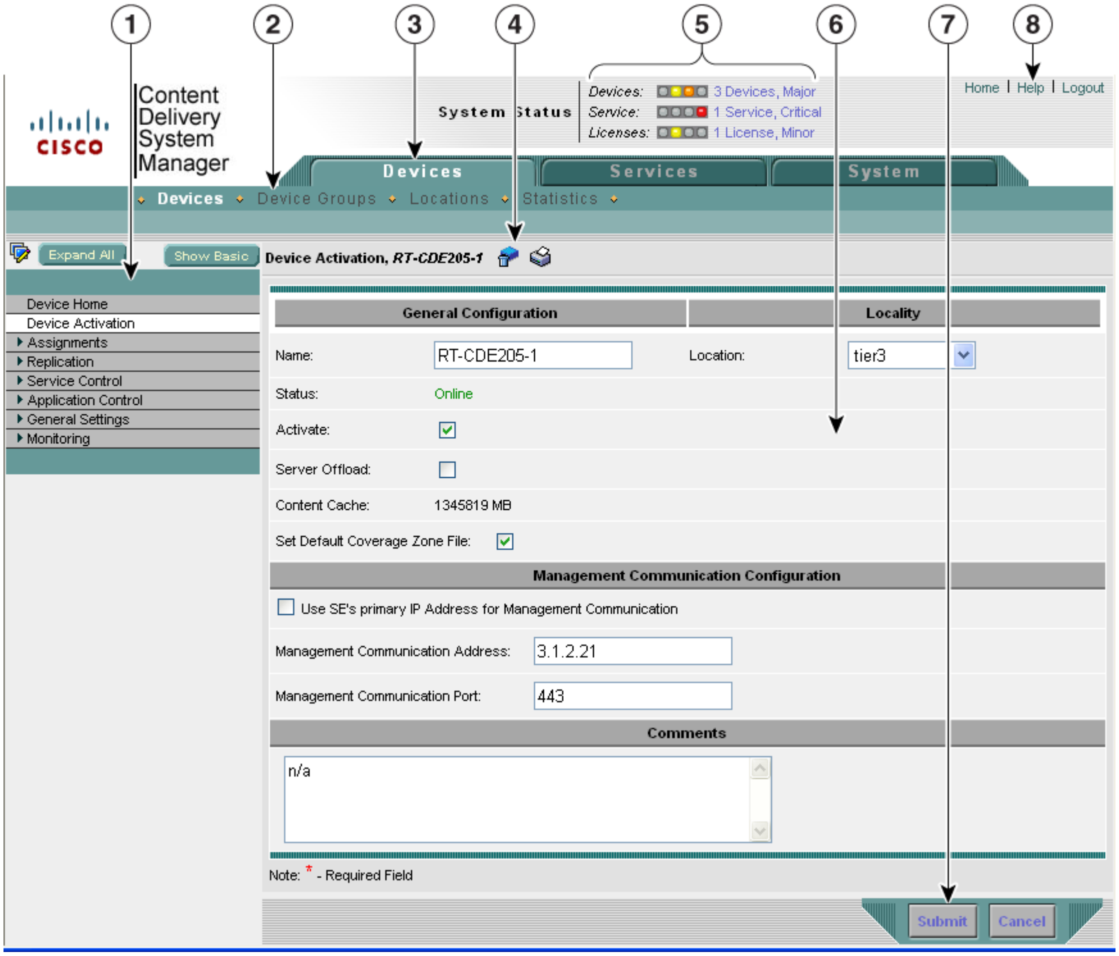
Note The built-in username is admin and the initial password is default. We strongly recommend that you change the built-in admin password as soon as possible. To do so, log in to the CLI of the CDSM device, and use the **username admin password <password>** global configuration command.

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

Navigating the CDSM

The following illustration shows the different elements in the CDSM GUI.

Figure 3-2 CDSM Graphical User Interface



Devices: 3 Devices, Major
Service: 1 Service, Critical
Licenses: 1 License, Minor

Device Activation, *RT-CDE205-1*

Name: RT-CDE205-1

Location: tier3

Status: Online

Activate: ☑

Server Offload: □

Content Cache: 1345819 MB

Set Default Coverage Zone File: ☑

□ Use SE's primary IP Address for Management Communication

Management Communication Address: 3.1.2.21

Management Communication Port: 443

n/a

Note: * - Required Field

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

The System Status bar, tab, 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.

For additional information on using the CDSM interface, see the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide (OL-23609-01)*.

Activating and Synchronizing Devices

As the OE administrator, you approve a device for use in the system by making it active. This security features prevents unauthorized devices from joining the system.

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

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

Caution All devices must be synchronized with each other for the system to work properly.

Activating and Setting NTP for Each Device

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

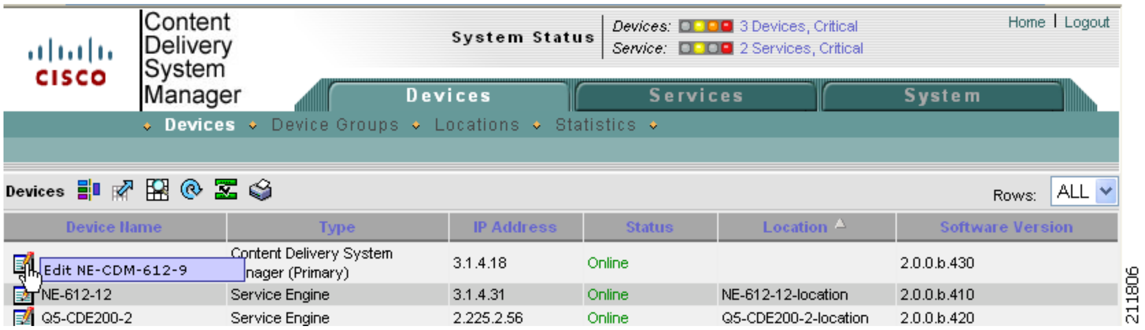
Devices > Devices > Assignments > Device Groups

Note From the Devices Table, you can activate all inactive devices by clicking the **Activate All Inactive SEs** icon.

To activate and synchronize a Service Engine (SE), do the following:

Step 1 From the CDSM home page, choose **Devices > Devices**. The Devices table is displayed listing all the registered SEs.

Figure 3-3 Devices Table Page – Edit Device



Devices: 3 Devices, Critical
Service: 2 Services, Critical

Devices Rows: ALL

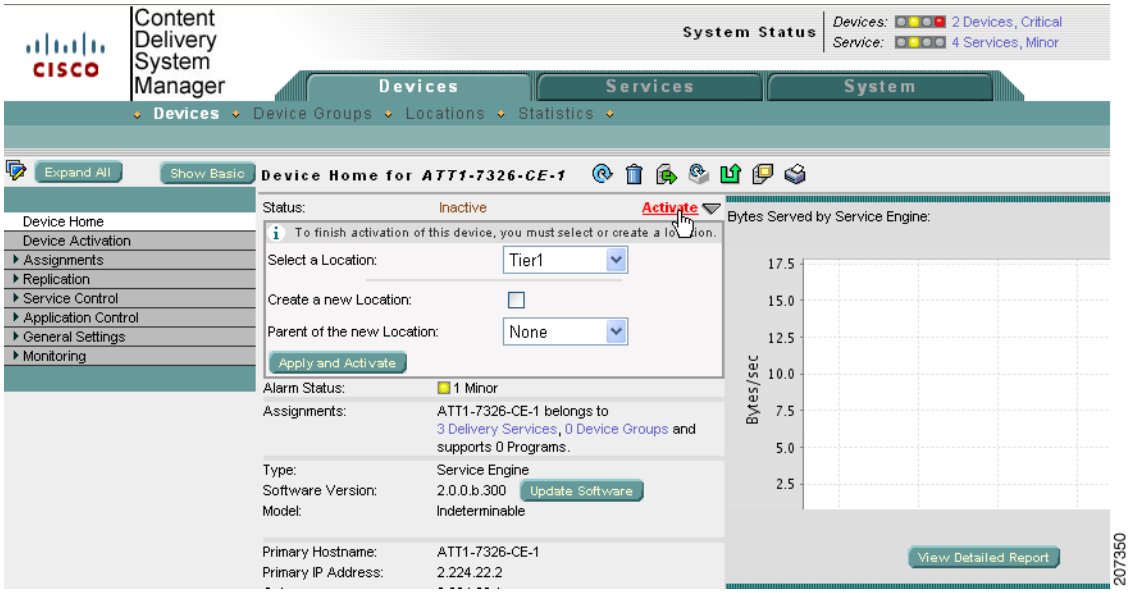
Device Name	Type	IP Address	Status	Location	Software Version
Edit NE-CDM-612-9	Content Delivery System nager (Primary)	3.1.4.18	Online		2.0.0.b.430
NE-612-12	Service Engine	3.1.4.31	Online	NE-612-12-location	2.0.0.b.410
Q5-CDE200-2	Service Engine	2.225.2.56	Online	Q5-CDE200-2-location	2.0.0.b.420

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

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

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

Figure 3-4 Devices Home Page – Location Dialog Box



Device Home for *ATT1-7326-CE-1*

Status: Inactive

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

Select a Location: Tier1

Create a new Location: □

Parent of the new Location: None

Alarm Status: 1 Minor

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

Type: Service Engine

Software Version: 2.0.0.b.300

Model: Indeterminable

Primary Hostname: ATT1-7326-CE-1

Primary IP Address: 2.224.22.2

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

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

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

- If you have already created locations, you can choose a location from the Location drop-down list.
- To create a default location that 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 new location.
- Because of the NAS mount requirement, all OE nodes must be in the root location, and therefore must have level "1" and parent "None."

Step 5 Click **Apply** and then click **Activate**.

The status of the device shows "pending" until the device is activated. This may take a few minutes.

Step 6 To display the top-level Table of Contents, click the **Show All** button above the Contents pane.

Step 7 From the left-panel menu, select **General Settings > Network > NTP**. The NTP Settings page is displayed.

Step 8 Check the **Enable** check box and enter the IP address or hostname of each NTP server. Use a space to separate each server.

Step 9 Click **Submit** to save your settings.

Note The activation and NTP server settings must be completed for each SE, OFAM, 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.

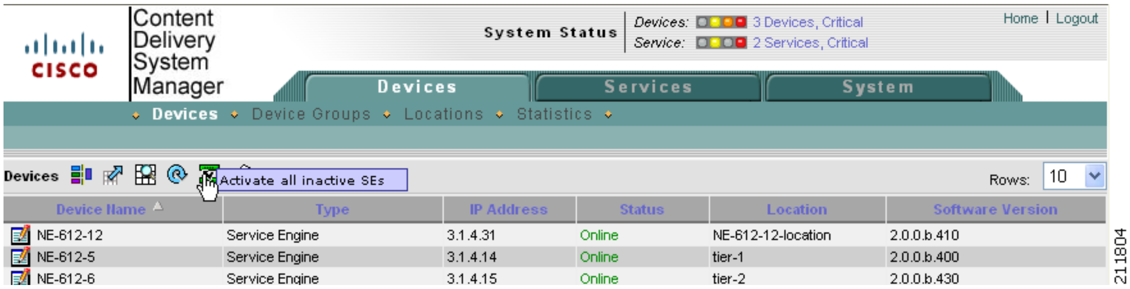
For more detailed information about activating devices and configuring locations and NTP servers, see the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide (OL-23609)*.

Activating All Inactive Service Engines

To activate all inactive SEs, do the following:

Step 1 From the CDSM home page, choose **Devices > Devices** and click the **Activate All Inactive SEs** icon.

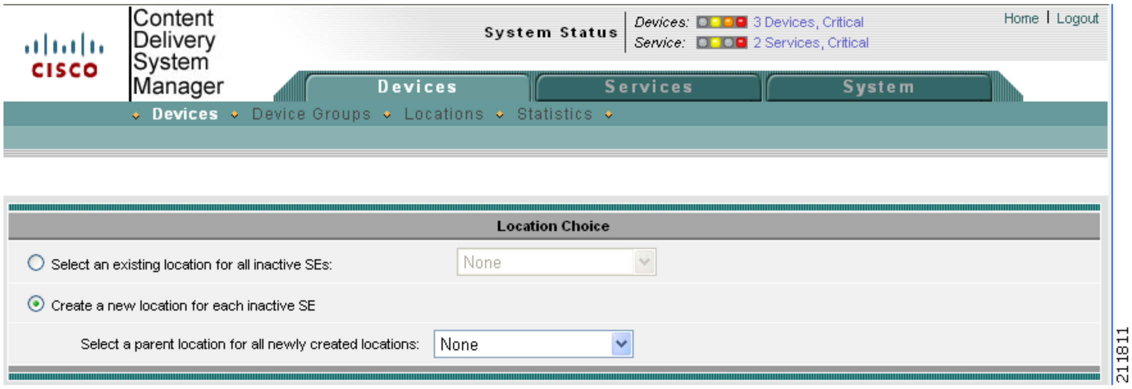
Figure 3-5 Devices Table Page – Activate All Inactive Service Engines


cisco
Content Delivery System Manager
System Status
Devices: 3 Devices, Critical
Service: 2 Services, Critical
Home | Logout
Devices
Services
System
Devices
Device Groups
Locations
Statistics
Devices
Activate all inactive SEs
Rows: 10
211804

Device Name	Type	IP Address	Status	Location	Software Version
NE-612-12	Service Engine	3.1.4.31	Online	NE-612-12-location	2.0.0.b.410
NE-612-5	Service Engine	3.1.4.14	Online	tier-1	2.0.0.b.400
NE-612-6	Service Engine	3.1.4.15	Online	tier-2	2.0.0.b.430

The Location Choice page is displayed.

Figure 3-6 Location Choice Page



Location Choice

○ Select an existing location for all inactive SEs: None

● Create a new location for each inactive SE

Select a parent location for all newly created locations: None

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

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

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

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

Note All devices activated in this way need to have the NTP settings configured, as described previously in the Activating and Setting NTP for Each Device section.

Synchronizing Clocks for OE Devices

We recommend synchronizing the clocks for all devices involved in the OE. This helps to ensure that all timestamps in the AIM database are accurate and that all “update” and “sync” mechanisms function properly.

To synchronize the clocks for all OE devices, do the following:

Step 1 In SE, OFAM, and CDSM (in any sequence), configure the NTP server and time zone. For example:

```
NTP server 171.68.10.150
clock timezone PDT -7 0.
```

Step 2 From any Linux management console:

a. Open the NTP port in your firewall.

b. In /etc/ntp.conf, add the IP address of the NTP server wherever the server pool is listed.

c. In /etc/ntp/step-tickers, add the IP address of the NTP server.

d. Run “ntpdate -dv <ntp-server-ip-address>” to synchronize the clocks.

Note The synchronization process usually takes 10 to 15 minutes to complete.

e. When the synchronization process is complete, run “hwclock --systohc” so that the system will acquire the new time on reboot.

Step 3 On the CTM Windows server:

a. Navigate to **Control Panel > Date and Time > Internet Time > Change Settings**.

b. Enter the IP address of the NTP server as the time server.

c. Confirm that the **Synchronize...** checkbox is checked.

d. Click **Update Now**.

Upon reboot, the clocks for all OE devices will be synchronized to the specified NTP server.

Configuring the System and Devices

After you have completed activating and configuring the NTP servers for all the devices in the CDSM, you are ready to configure the OE for video content delivery.

Configuring the OE involves both system configuration tasks and device configuration tasks.

System Configuration Tasks

System configuration involves registering (uploading) the following files:

- Content Adaptation File — A user-defined content adaptation file must be uploaded to the CDSM. CDSM ships with a default Content Adaptation XML file (factory.xml), which defines the rules by which OE optimizes and transcodes video assets. If needed, the operator can register a non-default Content Adaptation File.
- NAS File — Must be created in an XML text editor, registered or uploaded to CDSM, and associated with a Content Origin (delivery service). All OE nodes (except CDSM) must access the NAS device for offline transcoded content. A NAS XML file is registered with the CDSM to specify how the NAS should be mounted to the OE nodes.

A sample NAS XML file is shown below.

```
<?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>
```

For complete instructions on creating NAS files, see “Creating NAS Files” in the *Cisco CDS-IS 2.6 Software Configuration Guide*.

Device Configuration Tasks

Device configuration involves configuring the SE and OFAM components of the OE as well as configuration of CTM.

The SE component of the OE has a single configurable component called the Web Engine. The Web Engine is the main processing component of the OE, and performs the actual video serving function.

The OFAM component of the OE has three configurable subcomponents:

- Asset Information Manager (AIM), the catalog manager for offline content
- Offline Manager (OM), the manager for offline transcoding and caching
- Fetcher, the subcomponent responsible for retrieval of video content

Each of these components is configurated individually through dedicated CDSM GUI pages.

Note Although multiple Web Engine nodes can communicate with a single AIM node, only one AIM node can communicate with an Offline Manager node, and only one Offline Manager node can communicate with a Fetcher node.

Cisco Transcode Manager (CTM) Server is an independent application that provides video transcoding services for the OE, and must be configured for correct interoperation with the OE.

Typical Configuration Workflow

The steps for configuring the OE are normally performed in the following sequence:

1. Configure the Web Engine

2. Configure the AIM
3. Configure the OM
4. Configure the Fetcher
5. Configure Access Control (Blacklist and Whitelist)
6. Configure Partner Group settings
7. Register the Content Adaptation File (optional)
8. Configure the CTM Server
9. Configure NAS Eviction
10. Configure Transaction Logging

After you complete the OE configuration, the CDSM checks your input to confirm that it is valid. If the input is valid, the CDSM sends the configuration data to the CMS agent in the affected device. The CMS agent will then save the configuration data to its database and execute the corresponding CLI commands to configure the affected device(s).

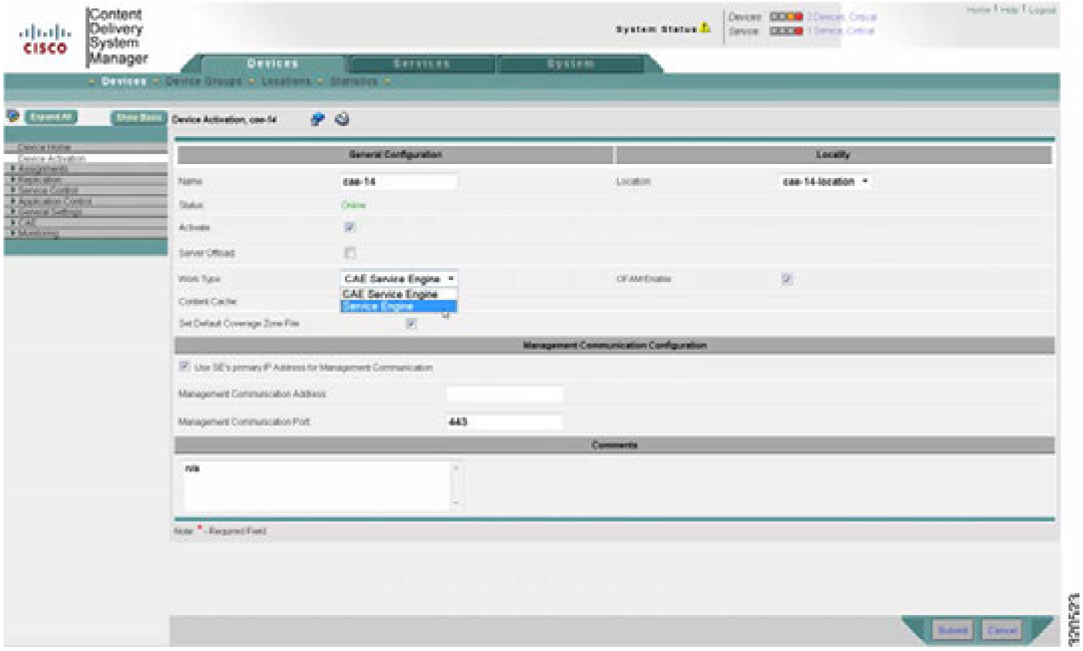
Note If you use CLI commands to configure devices, the CMS agent reports your changes to the CDSM so that the configuration data in CDSM and the CLI are kept consistent.

Service Engine Work Types

There are two work types for the CDS-IS Service Engine, namely CAE SE and the normal CDS-IS SE. You can switch the SE between these two modes from the Devices > Device activation page. To enable the CAE-related configuration, you would choose the CAE Service Engine work type.

Note When the normal Service Engine is selected, all CAE configuration settings are read-only and the corresponding CLI commands do not execute.

Figure 3-7 Device View and Work Type Settings



Device Activation, cae-14

General Configuration		Locality	
Name	cae-14	Location	cae-14-location
Status	Online		
Activate	☑		
Server Offload	☐		
Work Type	CAE Service Engine CAE Service Engine Service Engine	OF AM Enable	☑
Content Cache			
Set Default Coverage Zone File	☑		

Management Communication Configuration

☑ Use SE's primary IP Address for Management Communication

Management Communication Address

Management Communication Port 443

Comments

n/a

Note: * - Required Field

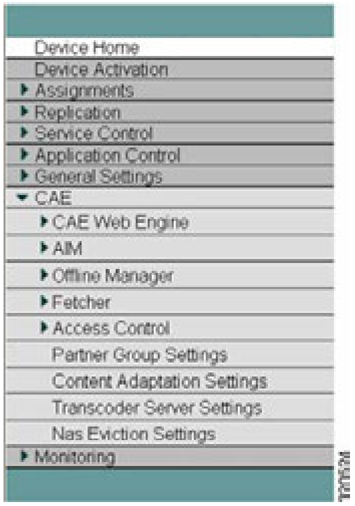
Using CDSM to Configure the OE

The CDSM user interface includes pages specifically designed to support OE configuration. All OE configuration is performed from the CDSM Devices tab by choosing **Devices > Device > CAE**.

Note Before using the CDSM to configure TCP server ports for the OE, confirm that the server ports you plan to use for OE are not used by other applications in your system.

Each page has a table of contents (TOC) menu, as shown in the following example. All OE configuration tasks are grouped under Devices > Device > CAE menu.

Figure 3-8 Devices > CAE Configuration Menu



Configuring the Web Engine

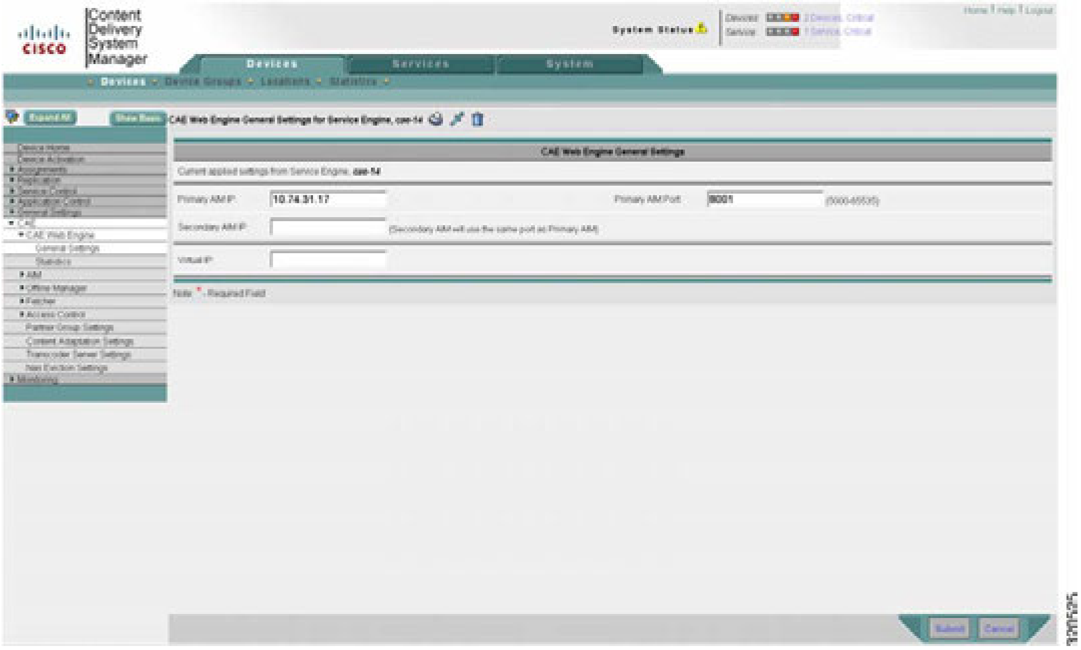
Configuration of the Web Engine involves configuring general settings. This section describes the procedure in detail.

General Settings

To configure general Web Engine settings, do the following:

Step 1 Choose **Devices > Devices > CAE > CAE Web Engine > General Settings**. The Web Engine General Settings page is displayed.

Figure 3-9 Web Engine General Settings



CAE Web Engine General Settings for Service Engine, cae-14

CAE Web Engine General Settings

Current applied settings from Service Engine, cae-14

Primary AIM IP: 10.74.31.17 Primary AIM Port: 8001 (5000-65535)

Secondary AIM IP: (Secondary AIM will use the same port as Primary AIM)

Virtual IP:

Note: * - Required Field

Step 2 Use this page to define the primary AIM information that the Web Engine will use to connect.

Note You can also specific a secondary AIM as a backup or redundant AIM. In that case, if the primary AIM should fail, the Web Engine automatically connects to the secondary AIM.

Configuring the AIM

AIM configuration covers following sections:

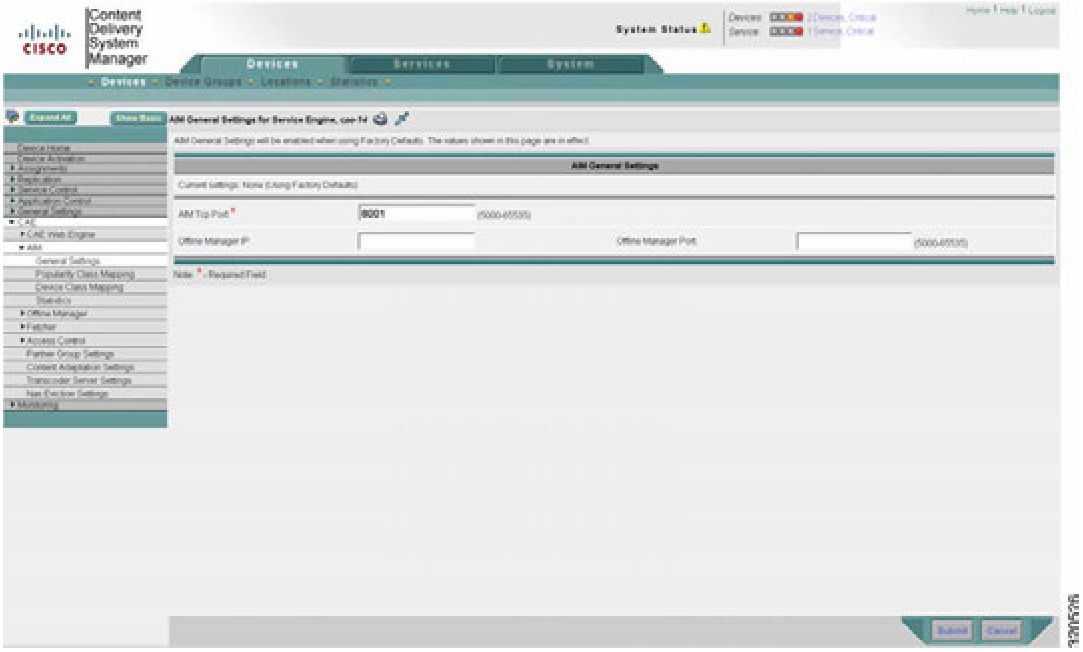
- General Settings
- Popularity Class Mapping
- Device Class Mapping

General Settings

To configure general AIM settings, do the following:

Step 1 Choose **Devices > Device > CAE > AIM > General Settings**. The General Settings page is displayed.

Figure 3-10 AIM General Settings



AIM General Settings for Service Engine, cae-14

AIM General Settings will be enabled when using Factory Defaults. The values shown in this page are in effect.

AIM General Settings

Current settings: None (Using Factory Defaults)

AIM Tcp Port * 8001 (5000-65535)

Offline Manager IP

Offline Manager Port (5000-65535)

Note: * - Required Field

Step 2 Define the AIM general settings, including:

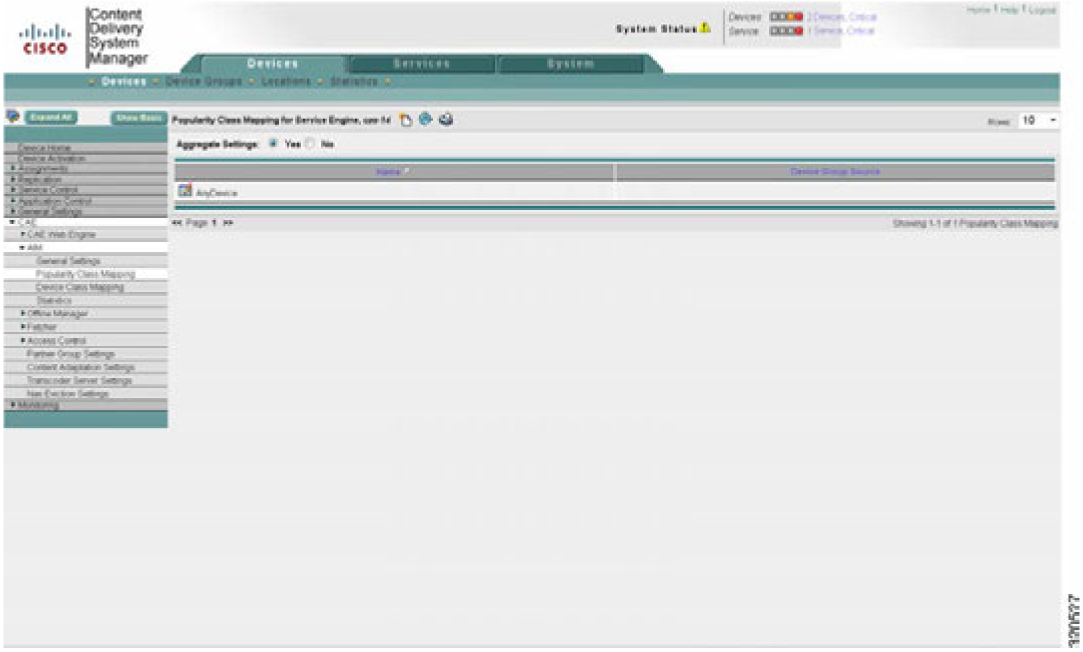
- The TCP server port the AIM process should listen to. The TCP server port is for Web Engine and is set to 8001 by default.
- The Offline Manager to which the AIM should connect. If Offline Manager IP and Offline Manager Port are left blank, the AIM uses defaults to connect to Offline Manager.

Popularity Class Mapping

To perform popularity class mapping, do the following:

Step 1 Choose **Devices > Device > CAE > AIM > Popularity Class Mapping**. The Popularity Class Mapping page is displayed.

Figure 3-11 AIM Popularity Class Mapping



Popularity Class Mapping for Service Engine, cae-1d

Aggregate Settings: ● Yes ○ No

Name	Device Group Source
AnyDevice	

Page 1

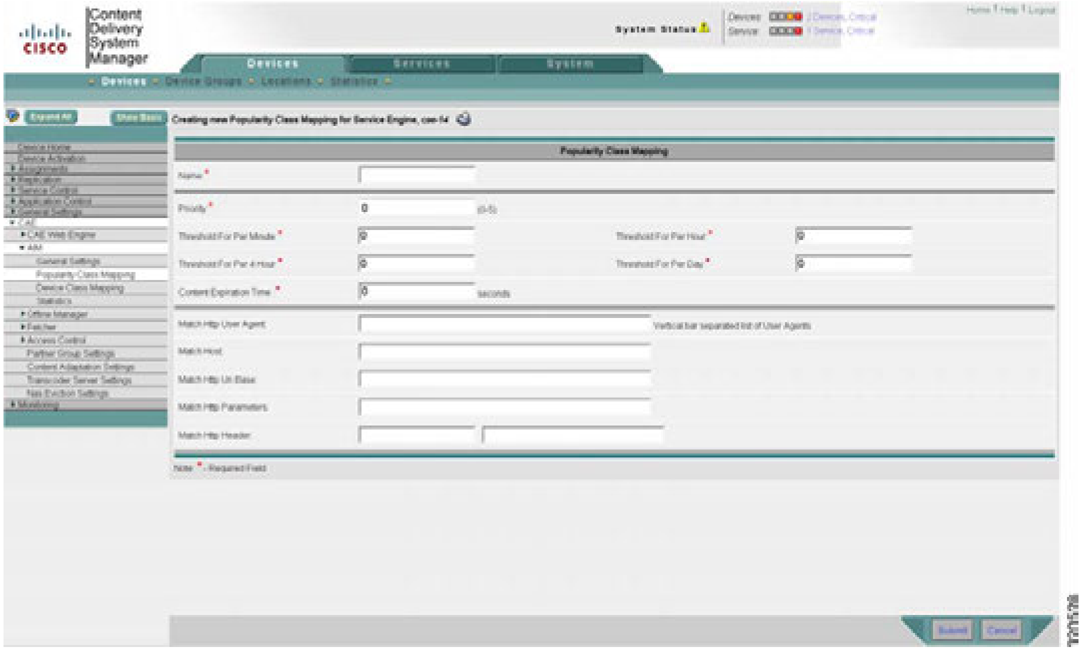
Showing 1-1 of 1 Popularity Class Mapping

Step 2 Define popularity settings as needed, such as the threshold for triggering offline adaptation.

- To edit an existing class, click the **Edit** icon next to the popularity class in the list.
- To create a new class, click the **Create New** icon ( ) in the task bar.

The AIM Popularity Class Mapping settings page is displayed.

Figure 3-12 Popularity Class Mapping Settings



Creating new Popularity Class Mapping for Service Engine, cae-54

Popularity Class Mapping

Name *

Priority * 0 (0-5)

Threshold For Per Minute * 0 Threshold For Per Hour * 0

Threshold For Per 4 Hour * 0 Threshold For Per Day * 0

Content Expiration Time * 0 seconds

Match Http User Agent Vertical bar separated list of User Agents

Match Host

Match Http Uri Base

Match Http Parameters

Match Http Header

Note: * - Required Field

Step 3 Complete the fields on this page as appropriate.

Table 3-1 AIM Popularity Fields

Field	Description
Name	Popularity class name.
Priority	Priority for the popularity class (range 1-5)
Threshold For Per Minute	Threshold value for hits per minute (range 1-2147483647).
Threshold For Per Hour	Threshold value for hits per hour (range 1-2147483647).
Threshold For Per 4 Hours	Threshold value for hits per 4 hours (range 1-2147483647).
Threshold for Per Day	Threshold value for hits per day (range 1-2147483647).
Current Expiration Time	Content expiration time in seconds (range 1-2147483647).
Match Http User Agent	List of User Agents, with list items separated by a vertical bar.
Match Host	Host in HTTP header, specified in normal string format.
Match Http Uri Base	The uribase from Request-URI.
Match Http Parameters	Parameters in Request_URI, such as id, format, etc. The value can can specified either in normal string or reg-exp string format. For example, either ".*(id=.+)\&" or ".*(key=.+)\&" will match and collect "id=e8996ff05f5c" and "key=ytal" from Request-URI.
Match Http Header	User-specified header name in HTTP GET messages.

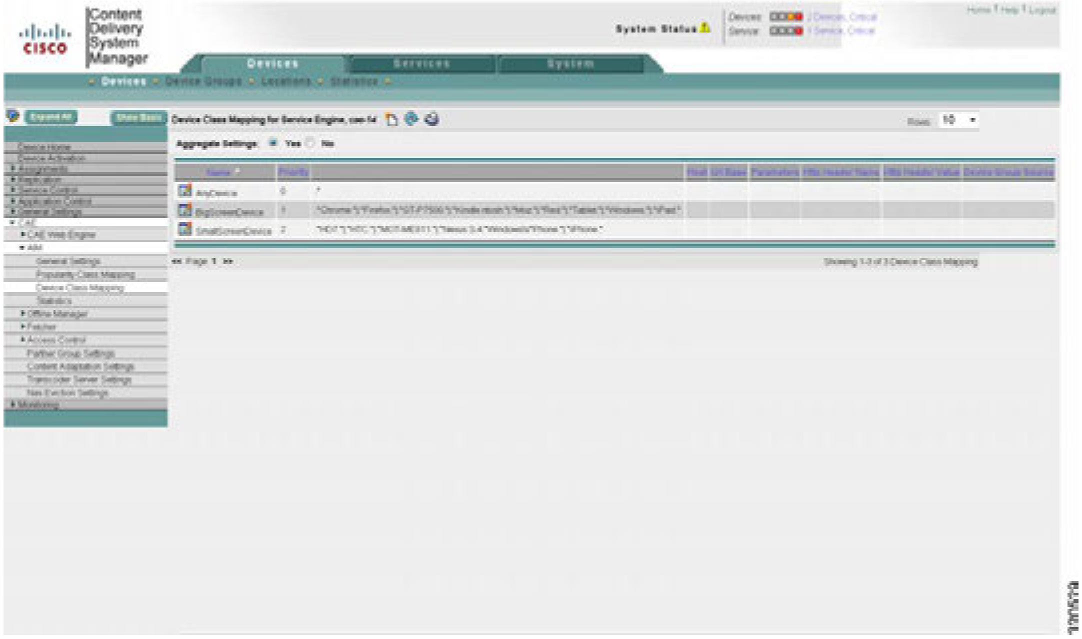
Note Required fields are marked by an asterisk (*).

Device Class Mapping

To perform device class mapping, do the following:

Step 1 Choose **Devices > Device > CAE > AIM > Device Class Mapping**. The Device Class Mapping page is displayed.

Figure 3-13 AIM Device Class Mapping



Device Class Mapping for Service Engine, cae-54

Rows: 10

Aggregate Settings: ● Yes ○ No

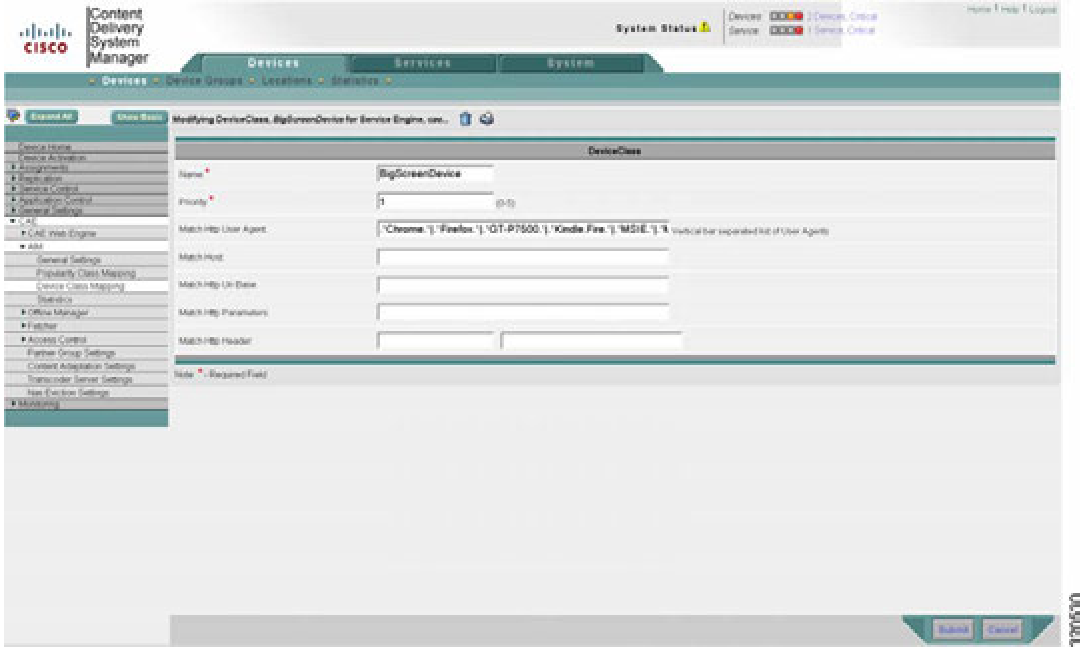
Name	Priority		Host	Url Base	Parameters	Http Header Name	Http Header Value	Device Group Source
AnyDevice	0	*						
BigScreenDevice	1	"Chrome "|"Firefox "|"GT-P7500 "|"Kindle ebook "|"Moz "|"Pad "|"Tablet "|"Windows "|"iPad "						
SmallScreenDevice	2	"HD7 "|"HTC "|"MOT-ME811 "|"Nexus S 4 "Windows*Phone "|"iPhone "						

Page 1

Showing 1-3 of 3 Device Class Mapping

Step 2 Use this page to define popularity settings, such as match rules for triggering adaptation or video selection.

Figure 3-14 AIM Device Class Settings



Modifying DeviceClass, BigScreenDevice for Service Engine, cae...

DeviceClass

Name* BigScreenDevice

Priority* 1 (0-5)

Match Http User Agent 'Chrome.'|'Firefox.'|'GT-P7500.'|'Kindle Fire.'|'MSIE.'|'t Vertical bar separated list of User Agents

Match Host

Match Http Uri Base

Match Http Parameters

Match Http Header

Note: * - Required Field

Step 3 Complete the fields on this page as appropriate.

Table 3-2 Device Class Fields

Field	Description
Name	Class name string
Priority	Number used to select the device class when multiple classes qualify. The higher the number, the higher the priority.
Match Http User Agent	User Agent in HTTP header. The value can be specified in either normal string or reg-exp string format.
Match Http Host	Host in HTTP header. The value can be specified in either normal string or reg-exp string format.
Match Http Uri Base	The uribase from Request_URI
Match Http Params	Parameters in Request_URI, such as id, format, etc. The value can can specified either in normal string or reg-exp string format. For example, either ".*(id=.+)\&" or ".*(key=.+)\&" will match and collect "id=e8996ff05f5c" and "key=ytal" from Request-URI.
Match Http Header	User-specified header name in HTTP GET or POST messages.

Note Required fields are marked by an asterisk (*).

Configuring the Offline Manager

The OM is a process with external interfaces to AIM, Fetcher, and the CTM Server. The interfaces with AIM and Fetcher are Inter-Process Communication (IPC) messages that are exchanged over a TCP connection. The interface with CTM Server is made through an HTTP REST API, in which an XML message body is transported through the HTTP protocol.

The OM acts as both an HTTP client and an HTTP server. As an HTTP client, it submits HTTP POST transcoding job requests to the CTM Server. The CTM Server has an HTTP POST asynchronous job status notification mechanism that informs its application whether the submitted transcoding job was successfully performed. This requires that the OM act essentially as an HTTP server.

You can perform all OM configuration through the CDSM GUI or by using the CLI. The only exception is NAS configuration, which can only be performed through the CDSM GUI.

Note Where both CDSM and CLI methods exist for a procedure, they are equivalent and synchronized. For consistency, we recommend the use of the CDSM GUI if VDS-IS is also installed.

The following optional configurations are available for OM:

- General Settings
- Fetcher Settings
- Statistics (view only)

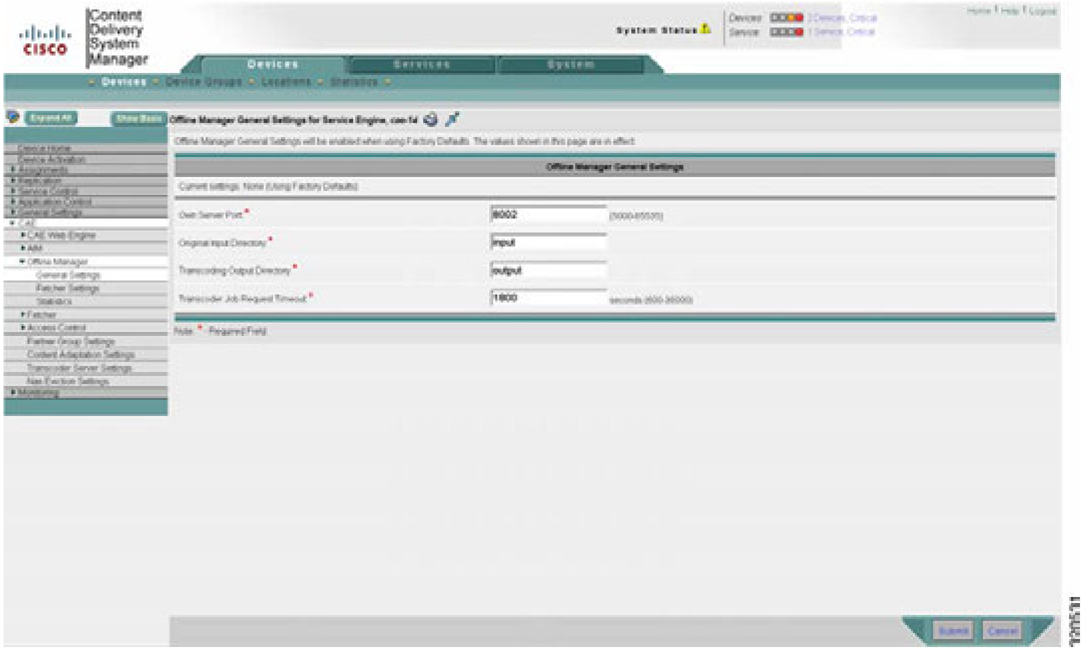
The following sections describe these procedures in detail.

Configuring OM General Settings

To configure OM general settings, do the following:

Step 1 Choose **Devices > Device > CAE > Offline Manager > General Settings**. The OM General Settings page is displayed.

Figure 3-15 OM General Settings



Offline Manager General Settings for Service Engine, cae-1d

Offline Manager General Settings will be enabled when using Factory Defaults. The values shown in this page are in effect.

Offline Manager General Settings

Current settings: None (Using Factory Defaults)

Own Server Port:* 8002 (5000-65535)

Original Input Directory:* input

Transcoding Output Directory:* output

Transcoder Job Request Timeout:* 1800 seconds (600-36000)

Note: * Required Field

Step 2 Complete the fields on this page as appropriate.

Table 3-3 General Settings Fields

Field	Description
Own Server Port	IPC TCP listening port for the AIM.
Original Input Directory	Location where Fetcher saves its downloaded original files.
Transcoding Output Directory	Location where CTM Server saves transcoded files.
Transcoder Job Request Timeout	Time that the OM waits for each transcoding job request.

Note Required fields are marked by an asterisk (*).

Default settings for each parameter are in place, but can be modified as follows to suit the needs of each deployment.

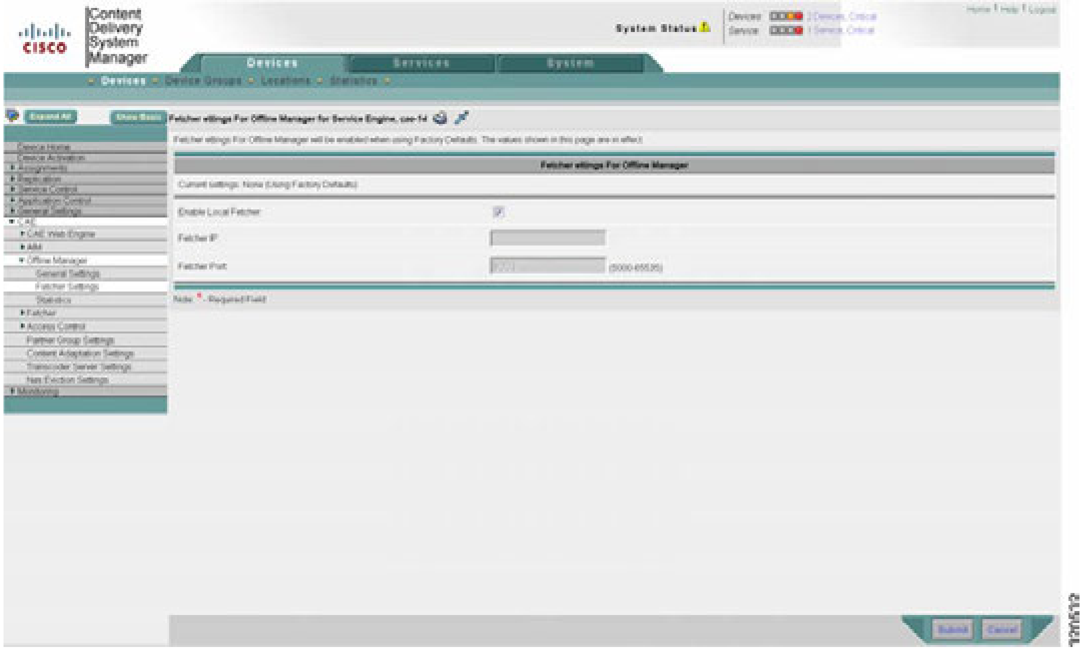
Configuring OM Fetcher Settings

Use the OM Fetcher Settings page to specify which Fetcher process the OM should use. By default, the OM always connects to a local Fetcher - that is, one running on the same node. However, you can choose to use an external Fetcher by entering its corresponding IP address and port, as follows.

To configure OM Fetcher settings, do the following:

Step 1 Choose **Devices > Device > CAE > Offline Manager > Fetcher Settings**. The OM Fetcher Settings page is displayed.

Figure 3-16 OM Fetcher Settings



Fetcher ettings For Offline Manager for Service Engine, cae-14

Fetcher ettings For Offline Manager will be enabled when using Factory Defaults. The values shown in this page are in effect.

Fetcher ettings For Offline Manager

Current settings: None (Using Factory Defaults)

Enable Local Fetcher ☑

Fetcher IP

Fetcher Port (5000-65535)

Note: * - Required Field

Step 2 Complete the fields on this page as appropriate.

Table 3-4 Fetcher Settings Fields

Field	Description
Enable Local Fetcher	Indicates that the Fetcher to which the OM should connect is on the same node as the OM. Enabled by default.
Fetcher IP	The IP address of the Fetcher.
Fetcher Port	The Fetcher port assignment. The default is 8003.

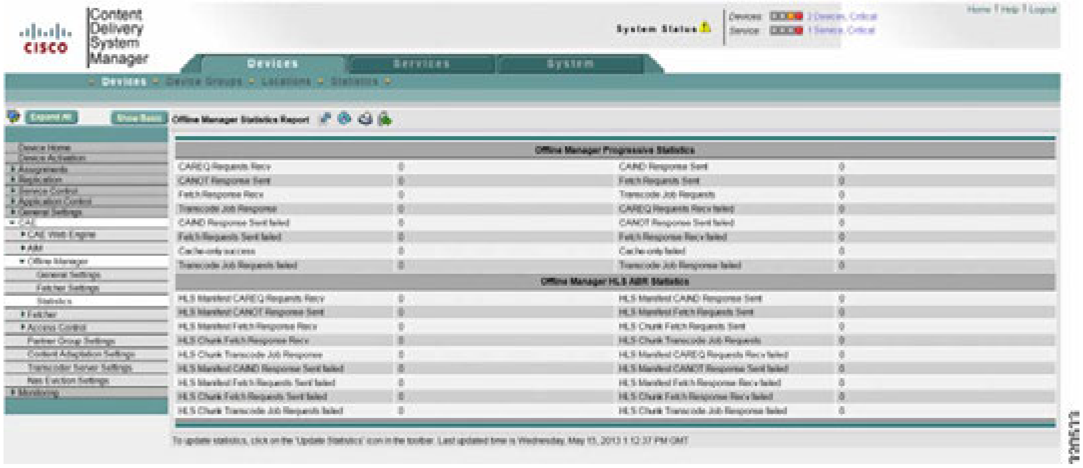
Note Required fields are marked by an asterisk (*).

Reviewing OM Statistics

To review OM statistics, do the following:

Step 1 Choose **Devices > Device > CAE > Offline Manager > Statistics**. The OM Statistics page is displayed.

Figure 3-17 OM Statistics



Offline Manager Progressive Statistics			
CAREQ Requests Recv	0	CAIND Response Sent	0
CANOT Response Sent	0	Fetch Requests Sent	0
Fetch Response Recv	0	Transcode Job Requests	0
Transcode Job Response	0	CAREQ Requests Recv failed	0
CAIND Response Sent failed	0	CANOT Response Sent failed	0
Fetch Requests Sent failed	0	Fetch Response Recv failed	0
Cache-only success	0	Cache only failed	0
Transcode Job Requests failed	0	Transcode Job Response failed	0
Offline Manager HLS ABR Statistics			
HLS Manifest CAREQ Requests Recv	0	HLS Manifest CAIND Response Sent	0
HLS Manifest CANOT Response Sent	0	HLS Manifest Fetch Requests Sent	0
HLS Manifest Fetch Response Recv	0	HLS Chunk Fetch Requests Sent	0
HLS Chunk Fetch Response Recv	0	HLS Chunk Transcode Job Requests	0
HLS Chunk Transcode Job Response	0	HLS Manifest CAREQ Requests Recv failed	0
HLS Manifest CAIND Response Sent failed	0	HLS Manifest CANOT Response Sent failed	0
HLS Manifest Fetch Requests Sent failed	0	HLS Manifest Fetch Response Recv failed	0
HLS Chunk Fetch Requests Sent failed	0	HLS Chunk Fetch Response Recv failed	0
HLS Chunk Transcode Job Requests failed	0	HLS Chunk Transcode Job Response failed	0

To update statistics, click on the 'Update Statistics' icon in the toolbar. Last updated time is Wednesday, May 15, 2013 1:12:37 PM GMT

Step 2 If needed, update the statistics display by clicking the **Update Statistics** ( ) button in the toolbar on this page.

Configuring the Fetcher

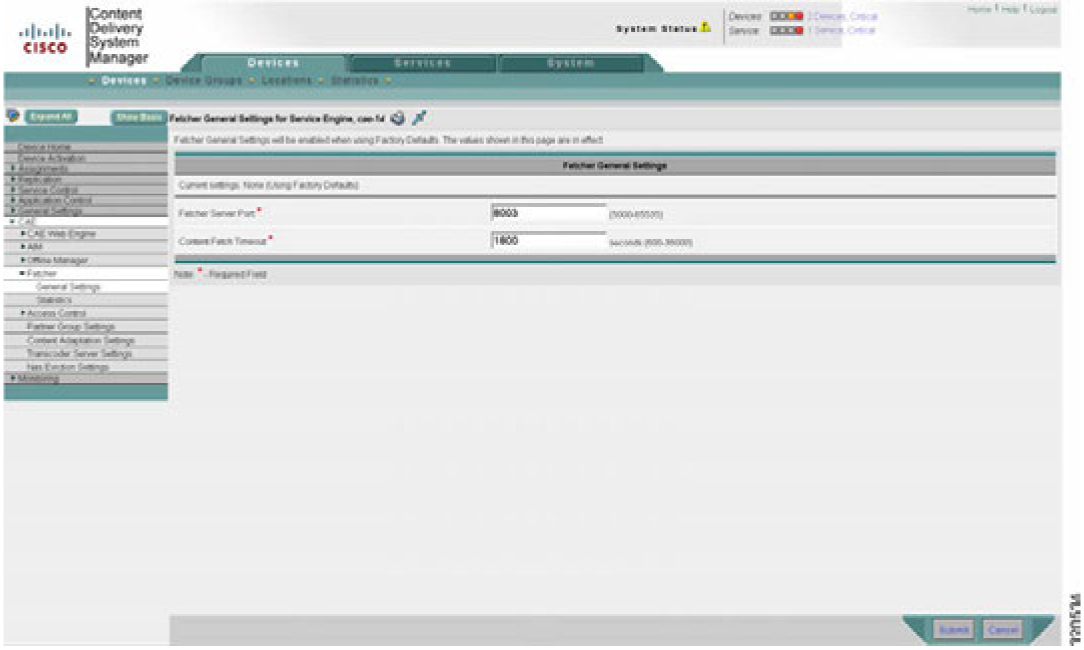
Configuration of the Fetcher involves configuring general settings. This section describes the procedure in detail.

General Settings

To configure general Fetcher settings, do the following:

Step 1 Choose **Devices** > **Devices** > **CAE** > **Fetcher** > **General Settings**. The Fetcher General Settings page is displayed.

Figure 3-18 Fetcher General Settings



Fetcher General Settings for Service Engine, cae-f4

Fetcher General Settings will be enabled when using Factory Defaults. The values shown in this page are in effect.

Fetcher General Settings

Current settings: None (Using Factory Defaults)

Fetcher Server Port* 8003 (5000-65535)

Content Fetch Timeout* 1800 seconds (600-36000)

Note: * - Required Field

Step 2 Complete the fields on this page as appropriate.

Table 3-5 Fetcher General Settings Fields

Field	Description
Fetcher Server Port	The port the Fetcher uses to listen to requests from the OM. The default is 8003.
Content Fetch Timeout	The timeout for content fetch in seconds. The default is 1800.

Note Required fields are marked by an asterisk (*).

Configuring Access Control

The AIM component manages a Blacklist and a Whitelist that can be used to identify content to be transcoded. The Blacklist identifies content that is not to be transcoded, while the Whitelist identifies content that is to be transcoded. The two lists can be referenced independently.

When either list is used, the AIM compares the Host, Referrer, Client IP, and User Agent strings in the incoming HTTP request (CRREQ) header, along with corresponding entries in other generic HTTP headers, first in the Blacklist (if used) and then in the Whitelist (if used). Appropriate action is then taken as follows:

- If the Blacklist is not configured or has no match for the HTTP message header, the header is passed to the Whitelist for comparison.
- If the Blacklist is configured and a match is found, the video request is bypassed, and the HTTP message header is not passed to the Whitelist.
- If the Whitelist is not configured or if a match is found in the Whitelist for the HTTP message header, transcoding is performed, and the choice of offline or online transcoding is made based on the information in the adaptation XML file.
- If the Whitelist is configured and no match is found, the video request is bypassed.

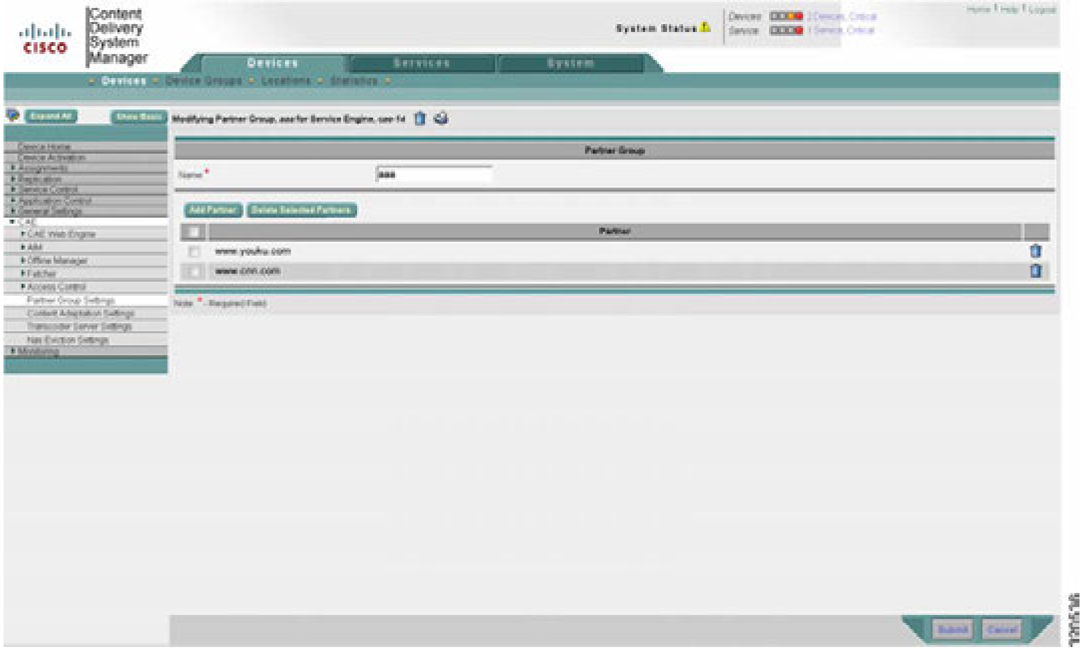
Note Blacklist and Whitelist configurations are processed only by the OFAM, so only the OFAM server requires Blacklist and Whitelist configurations. The decisions derived from this processing are passed to other system components as appropriate.

Configuring Partner Group Settings

You can add a partner group to the configuration as follows:

Step 1 Choose **Devices > Devices > CAE > Partner Group Settings**. The Partner Group Settings page is displayed.

Figure 3-19 Partner Group Settings



Modifying Partner Group, aaa for Service Engine, cae-14

Partner Group

Name * aaa

□	Partner
□	www.youku.com
□	www.cnn.com

Note: * - Required Field

Step 2 In the **Name** field, enter a name for the partner group.

Step 3 Click to select items from the **Partner** list to add to the group.

Step 4 Click **Add Partner** to add the selected partners to the group.

Step 5 Click **Submit** to save your entries, or click **Cancel** to abort the operation.

Note To delete partners from the group, select the partners to be deleted and click **Delete Selected Partners**.

Configuring 3GP and 3G2 Settings

The factory default XML file is preconfigured to enable 3GP and 3G2 caching. The following pattern matching rules and actions apply:

```
<PatternListGrp id="3GP">
      <ContentSourceType>3gp</ContentSourceType>
    </PatternListGrp>

<PatternListGrp id="3G2">
      <ContentSourceType>3g2</ContentSourceType>
    </PatternListGrp>
```

These pattern rules will match the following actions respectively

```
<SetParameter matchGroup="3GP">
      <Action>Cache_Only</Action>
    </SetParameter>

    <SetParameter matchGroup="3G2">
      <Action>Cache_Only</Action>
    </SetParameter>
```

The action Cache_Only is defined as follows:

```
<Rule_SetAction name="Cache_Only">
      <SetParameter  name="Progressive-Video">
        <CacheOnly>1</CacheOnly>
      </SetParameter>
```

Cache-only action is enabled or disabled by setting or resetting the <CacheOnly> tag. A **1** indicates that Cache_Only is enabled.

AIM Popularity for 3GP and 3G2 Video

The AIM popularity threshold configuration is also used as a trigger for 3GP and 3G2 video caching, and the OE uses the same ordering rules for serving popular content. The first access of a 3GP or 3G2 video available for offline serving is served to the client from the NAS. At the same time, the SE caches the video to its local cache, and any subsequent requests are then served from the SE's local cache.

Registering the Content Adaptation File (Optional)

The OFAM requires a Content Adaptation File to determine what action to take with regard to original video files downloaded by the Fetcher. The Content Adaptation File may include instructions for transcoding progressive video, applying pacing to a video stream, and modifying the HLS manifest file – for example, to delete an unwanted bit rate from the manifest file and insert a new bit rate with specific use conditions.

The first step in Content Adaptation File registration is to create an XML configuration file using a suitable text editor. After creating the XML file, you upload the file to the CDSM and then download the file to the SEs.

Note A sample Content Adaptation File is provided in the form of the factory default adaptation XML file, **factory.xml**. You cannot modify or delete this file, but you can add additional XML files. The device configuration determines which adaptation file is currently in effect.

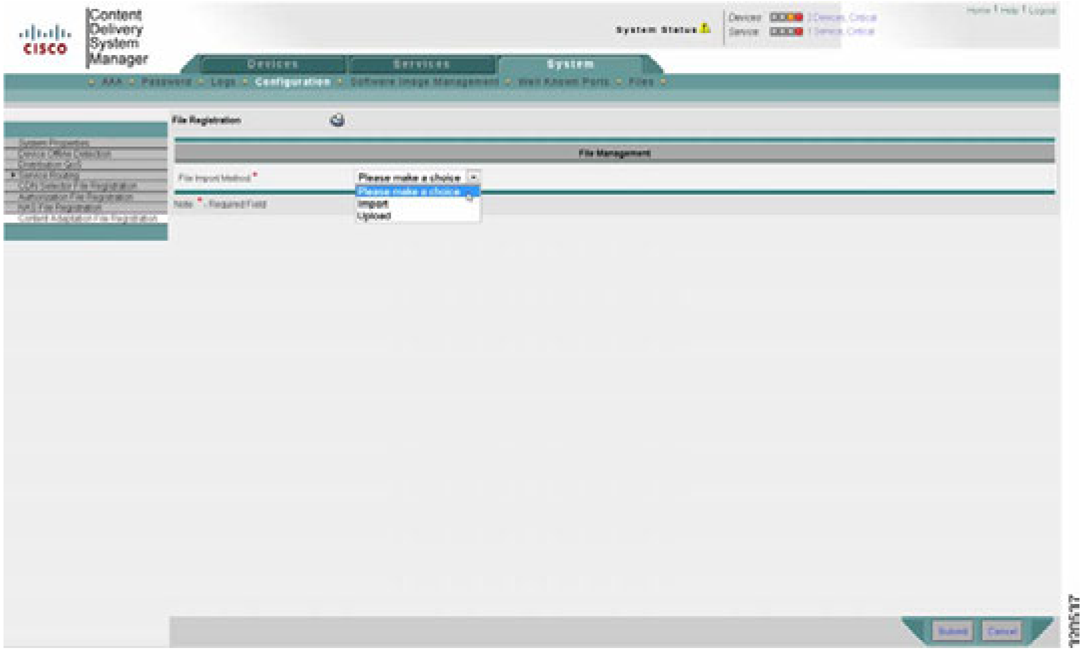
To register a content adaptation file, do the following:

Step 1 Create the Content Adaptation File according to the factory default adaptation XML file provided as an example.

Step 2 Choose **System > Configuration > Content Adaptation File Registration > Create** (click the file icon) to create the Content Adaptation XML file. The File Registration page is displayed.

Step 3 In the File Registration page, choose **Import** or **Upload** as appropriate to transmit the Content Adaptation Configuration File to the CDSM.

Figure 3-20 Content Adaptation File Registration Page



File Registration

File Management

File Import Method * Please make a choice

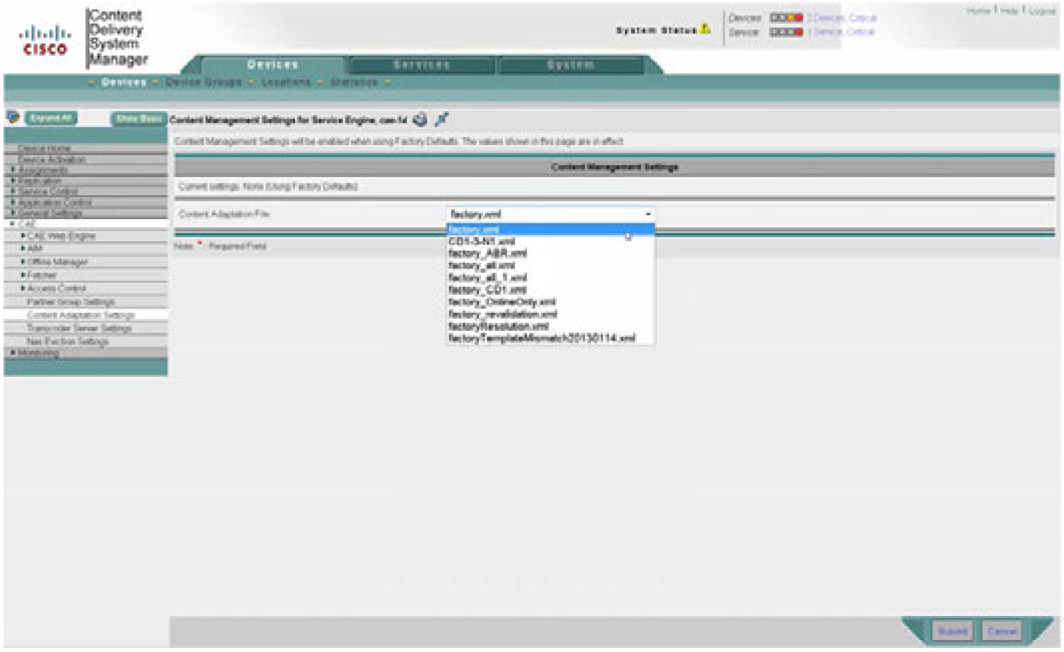
Please make a choice
Import
Upload

Note: * - Required Field

Step 4 Choose **Devices > CAE > Content Adaptation Settings**. The Content Management Settings page is displayed.

Step 5 Select the XML file to be downloaded to the SEs (**factory.xml** in the example shown below), then click **Submit** in the lower right corner of the page. CDSM downloads the XML file to the SEs.

Figure 3-21 Content Adaptation File Registration – Submit File



Content Management Settings for Service Engine, cae-1d

Content Management Settings will be enabled when using Factory Defaults. The values shown in this page are in effect.

Content Management Settings

Current settings: None (Using Factory Defaults)

Content Adaptation File: factory.xml

factory.xml
CD1-3-N1.xml
factory_ABR.xml
factory_all.xml
factory_all_1.xml
factory_CD1.xml
factory_OnlineOnly.xml
factory_revalidation.xml
factoryResolution.xml
factoryTemplateMismatch20130114.xml

Note: * - Required Field

Registering the NAS File

The NAS acts both as a centralized storage device and as an HTTP origin server (Web server) for the OE. As a storage device, the OM instructs the Fetcher process to save original content downloaded from an external Web server to a specified directory on the NAS. Similarly, the Offline Manager selects a NAS directory and filename for the Transcoder Server to store the transcoded content.

Because the OM is aware of the NAS info, it can generate a NAS-based HTTP URL for accessing the transcoded content. This URL is later saved to the AIM database.

Note Both the the IP address and the domain name are supported for NAS mounting.

As mentioned earlier, you can only configure the NAS through the CDSM. You must first prepare a NAS XML configuration file. For example, a file named “nas_mount.xml” can contain:

```
<?xml version="1.0" ?>
<CdsOrigin>
  <server name="CAE-nas" host="172.25.128.122" />
  <sourceNFS name="NFS" sharePoint="vol/vol0/home" access="rw" rsize="32768" maxRetry="10"
/>
  <localMount name="local" source="NFS" mountPoint="cae" order="fcfs" num-of-mounts="1"
serverList="CAE-nas" />
</CdsOrigin>
```

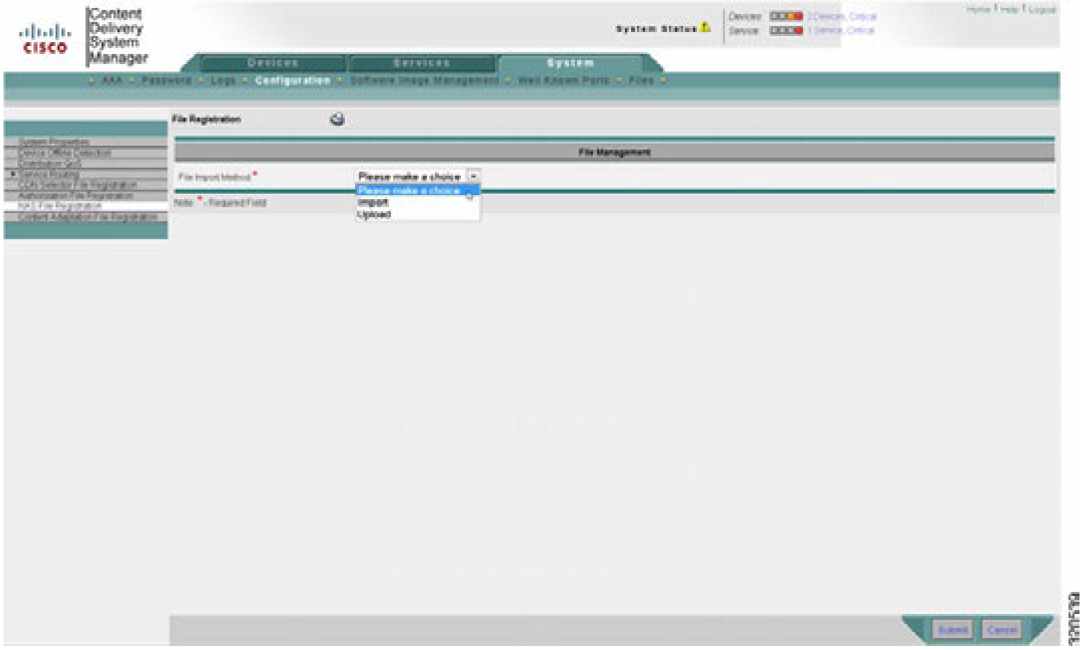
After creating the XML file, you can upload the file to the CDSM as follows:

Step 1 Choose **Systems > Configuration > NAS File Registration.**

Step 2 Click the **Create** (🗋) icon to create a new NAS file.

Step 3 Choose **Upload** or **Import** as appropriate.

Figure 3-22 NAS File Registration – Upload or Import

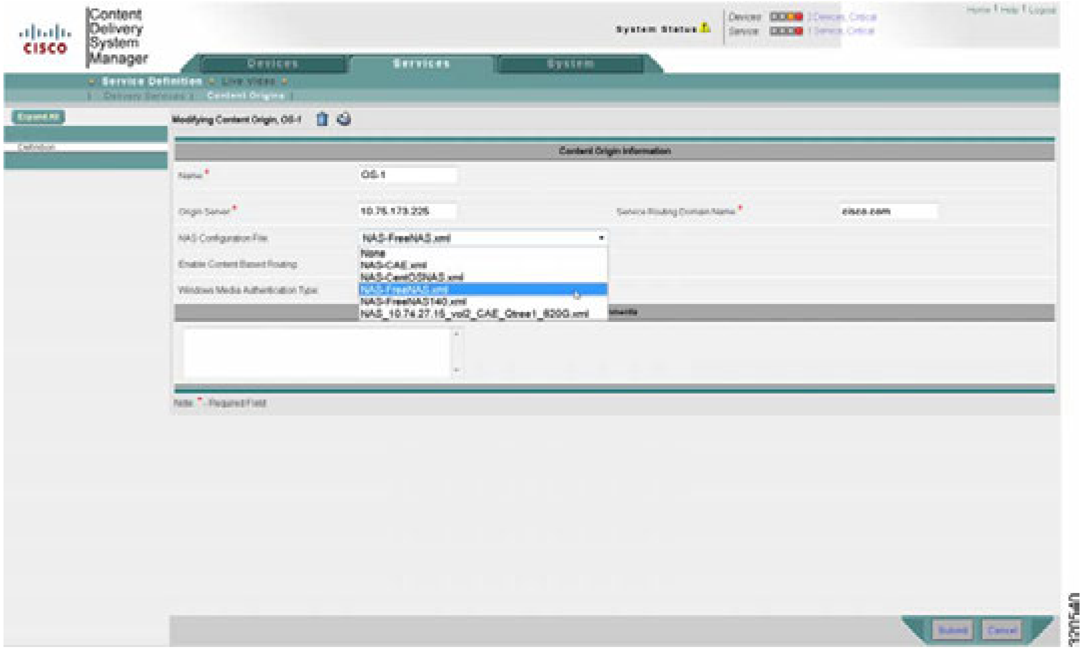


File Import Method*: Please make a choice

Note: * - Required Field

Step 4 Choose **Services > Content Origin > Definition > NAS XML File > Submit** to download the NAS file to SEs.

Figure 3-23 NAS File Registration – Download to SEs



Modifying Content Origin, OS-1

Content Origin Information

Name* OS-1

Origin Server* 10.75.173.226

Service Routing Domain Name* cisco.com

NAS Configuration File NAS-FreeNAS.xml

Enable Content Based Routing

Windows Media Authentication Type

Note: * - Required Field

Creating a Delivery Service and Location

For instructions on creating a delivery service and location, see the *Cisco Internet Streamer CDS 2.6 Software Configuration Guide (OL-23609).*

Configuring the Transcoder Server

Transcoder Server configuration is required for both the SE and OFAM components of the OE. Perform the following steps to configure the Transcoder Server IP address and port assignment and add related information as needed.

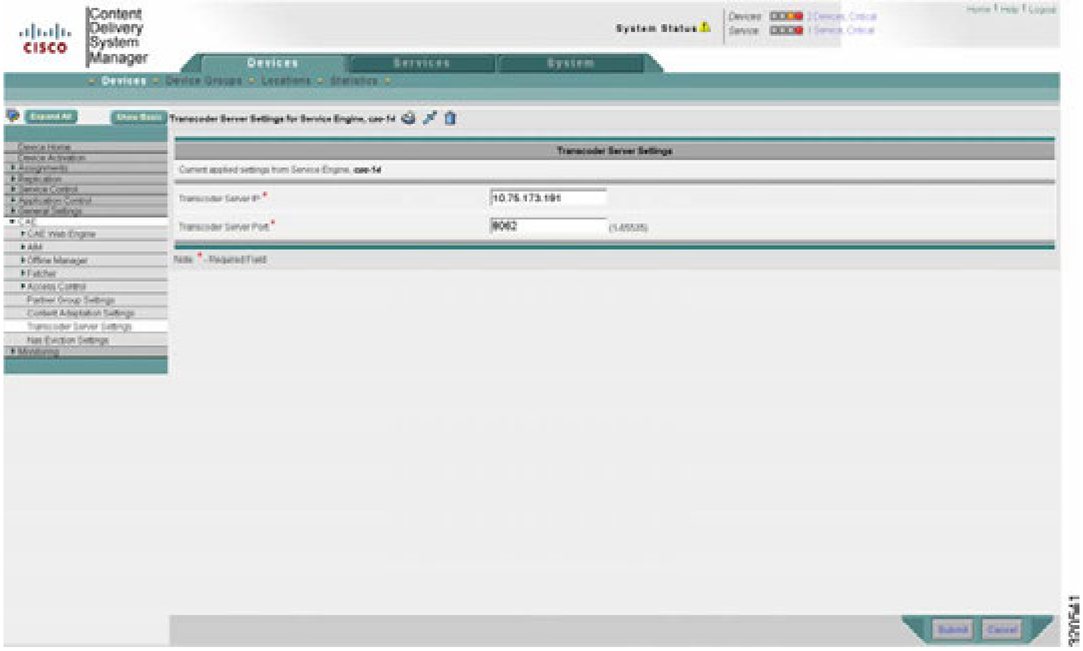
Tip Obtain the IP address of the Transcoder Server before performing this procedure, as it will be needed to complete the procedure. The default Transcoder port is 8062.

Note The IP address and port assignment for the Transcoder Server are mandatory.

To configure Transcoder Server settings from the Transcoder Settings page, do the following:

Step 1 Choose **Devices > Device > CAE > Transcoder Server Settings**. The Transcoder Server Settings page is displayed.

Figure 3-24 Transcoder Server Settings



Transcoder Server Settings for Service Engine, cae-14

Transcoder Server Settings

Current applied settings from Service Engine, cae-14

Transcoder Server IP *	10.75.173.191	
Transcoder Server Port *	8062	(1-65535)

Note: * - Required Field

Step 2 On this page, enter appropriate communication settings to enable the Web Engine and Offline Manager to submit transcoding jobs to the Transcoder Server.

Step 3 Click **Submit** to save your changes, or click **Cancel** to abort the operation.

Note The Transcoder Server stores all template files for video transcoding. An extensive set of pre-defined template files ships with the Transcoder product, so you may not need to edit these files or create new ones. But if this should become necessary, you can use the CTM Manager GUI to create, edit, and delete template files.

CTM Manager is a separate GUI-based management system that runs on the Transcoder Server. The CTM Manager also includes a set of APIs so that you can manage the Transcoder Server programmatically. See the *Cisco Transcode Manager User Guide v4.5* for further details.

Configuring NAS Eviction Settings

NAS eviction is the periodic deletion of old content stored on the NAS to ensure that there is always room for new content. Three settings control the triggering of the NAS eviction process:

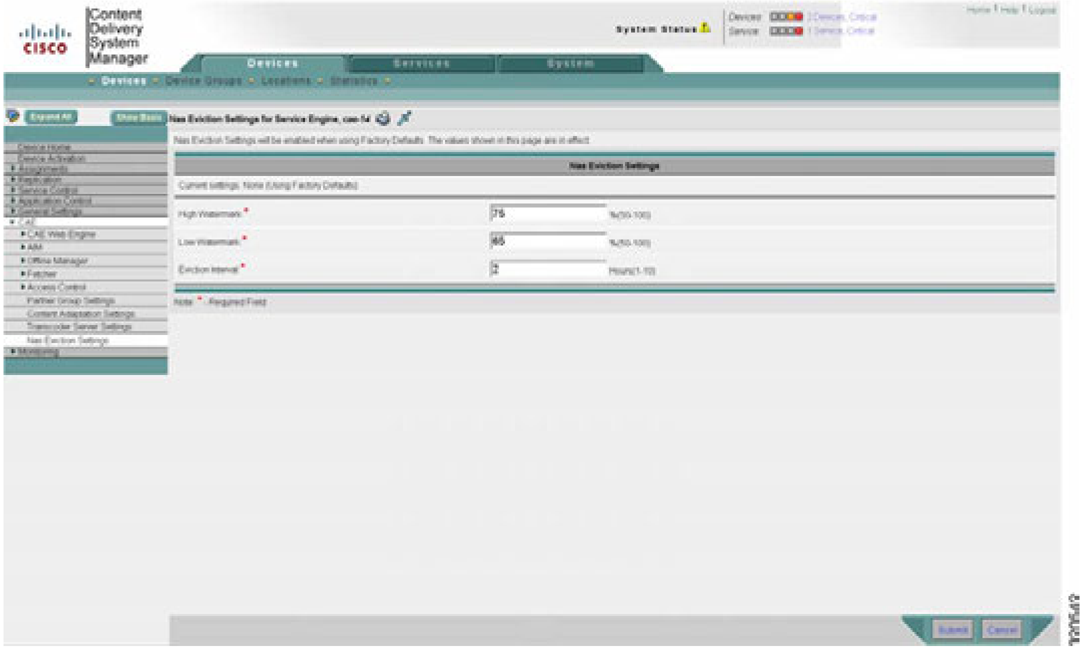
- High Watermark—The utilization percentage that triggers activation of NAS eviction
- Low Watermark—Tthe utilization percentage that triggers suspension of NAS eviction
- Eviction Interval—The number of hours between successive utilization checks

By default, NAS utilization is checked at Eviction Intervals of 2 hours. Then, NAS eviction is activated if the NAS has reached or exceeded a High Watermark of 75% utilization, or suspended if the NAS has reached or fallen below a Low Watermark of 65% utilization.

These settings can be modified to suit the needs of different deployments as follows:

Step 1 Navigate to **Devices > Device > CAE > NAS Eviction Settings**. The NAS Eviction Settings page is displayed.

Figure 3-25 NAS Eviction Settings Page



Nas Eviction Settings for Service Engine, cae-5d

Nas Eviction Settings will be enabled when using Factory Defaults. The values shown in this page are in effect.

Nas Eviction Settings

Current settings: None (Using Factory Defaults)

High Watermark: *	75	%(50-100)
Low Watermark: *	65	%(50-100)
Eviction Interval: *	2	Hours(1-10)

Note: * - Required Field

Step 2 Enter new values for **High Watermark**, **Low Watermark**, and **Eviction Interval** as needed.

Step 3 Click **Submit** to save your changes, or click **Cancel** to abort the operation.

Configuring Transaction Logging

The Transaction Logging feature records a log of significant system events, including a record of each video served, and saves it to the CAE-SE file system. You use the Transaction Log Settings page to enable Transaction Logging and define appropriate settings for your deployment.

The following settings are available on the Transaction Log Settings page:

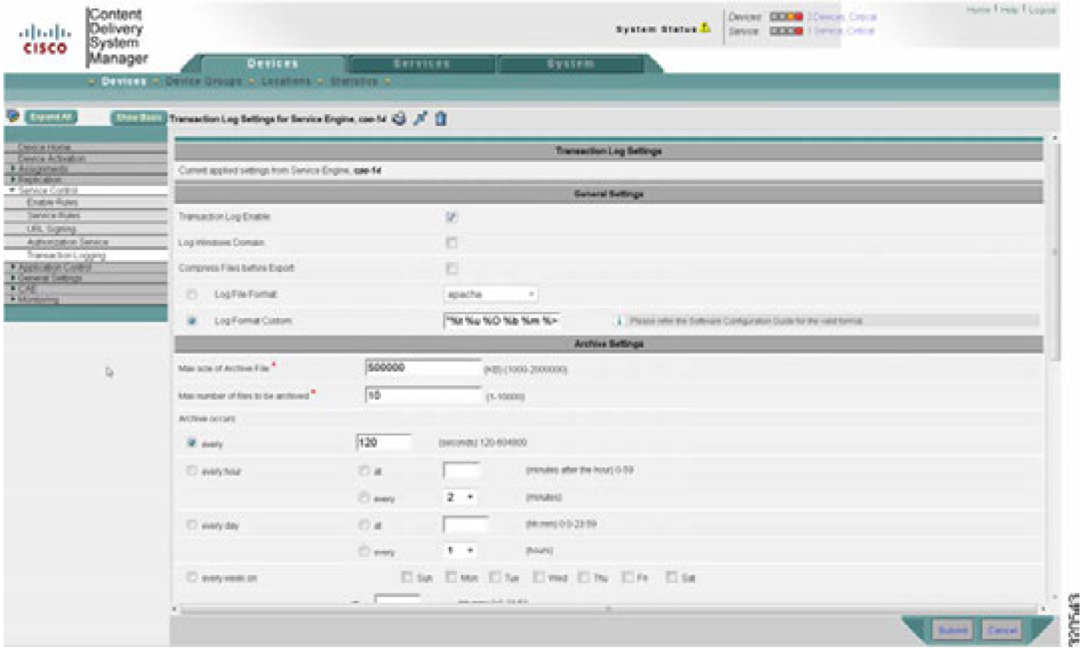
- Transaction Log Enable—Check to enable or clear to disable
- Log Windows Domain—Check to enable or clear to disable
- Enable Export—Check to enable or clear to disable
- Export occurs—Define the interval for Transaction Log export
- FRP Export Server—Name, credentials, and location for each export server

- Enable Windows Media Settings—Check to enable or clear to disable
- Log File Format—wms-41

To access the Transaction Log Settings page, do the following:

Step 1 Navigate to **Devices > Device > Service Control > Transaction Logging**. The Transaction Log Settings page is displayed.

Figure 3-26 Transaction Log Settings Page



Transaction Log Settings for Service Engine, cae-14

Transaction Log Settings

Current applied settings from Service Engine, cae-14

General Settings

Transaction Log Enable ☑

Log Windows Domain □

Compress Files before Export □

○ Log File Format apache

● Log Format Custom "%t %u %O %b %m %>

Please refer the Software Configuration Guide for the valid format

Archive Settings

Max size of Archive File* 500000 (KB) (1000-2000000)

Max number of files to be archived* 10 (1-10000)

Archive occurs

● every 120 (seconds) 120-604800

○ every hour ○ at (minutes after the hour) 0-59

○ every 2 (minutes)

○ every day ○ at (hh:mm) 0:0-23:59

○ every 1 (hours)

○ every week on □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Step 2 Update the fields on this page as needed to configure Transaction Logging for your deployment.

Step 3 Click **Submit** to save your changes, or click **Cancel** to abort the operation.

CHAPTER 4

Managing and Monitoring the VDS-OE

Overview

This chapter describes the functions available in the CDSM and elsewhere for managing and monitoring the OE and related operations.

Management

The CDSM can be used to manage the OE as well as VDS-IS, if also installed. The CDSM features a GUI interface and a synchronized command line interface (CLI) for browser-based or command-line driven network management and device monitoring.

The OE can also be managed using an XML or CLI/API interface. Existing UCS platform APIs can be adopted for platform specific management.

NAS Management

The NAS is managed by the CdsOrigMgr process. The process mounts the NAS at a proper share point, periodically (every 5 seconds) monitors the NAS accessibility, and writes an /etc/nasinfo file. The Offline Manager reads the /etc/nasinfo file to gather the NAS related information. The NAS is mounted as read-only. For OE, however, the NAS must be mounted as read-write. Dynamic NAS mount changes are supported by the Offline Manager.

The Offline Manager uses a specific convention to organize the original (input) and transcoded (output) files.

Input Location

By default, input files are placed in the following location:

$NAS_share_dir/$input_dir/$YYYY_MM_DD/$SE_hostname/$device_class/$url_domain/$asset_descriptor.$container_type

For example:

```
/state/export/NAS/172.25.128.122/cae/0/input/2012_04_08/sjst68/iPad/172.25.128.81/
ab8f76df002012031200323500e228e1.flv
```

Where:

- $NAS_share_dir – "/state/export/NAS/172.25.128.122/cae/0/". This portion is configurable based on the NAS XML mounting file.
- $input_dir – "input"; This portion is configurable using either CLI or CDSM.
- $YYYY_MM_DD – "2012_04_08"
- $SE_hostname – "sjst68"
- $device_class – "iPad"
- $url_domain – "172.25.128.81"
- $asset_descriptor – "ab8f76df002012031200323500e228e1"
- $container_type – "flv"

Note For HLS ABR, only the master(parent) manifest file is named using the $asset_descriptor.m3u8. Its associated chunk (.ts) files are placed in a subfolder of the parent manifest file folder.

Output Location

By default, output files are placed in the following location:

$NAS_share_dir/$output_dir/$YYYY_MM_DD/$SE_hostname/$url_domain/$path/$asset_descriptor +$device_class+$Adapatation_Profile_index.$container_type

For example:

```
/state/export/NAS/172.25.128.122/cae/0/output/2012_04_05/p-cae/sjst81.cisco.com/sample
/6d2f80bc00201109081355020052162f+iPhone4+0.mp4
```

Where:

- $NAS_share_dir – "/state/export/NAS/172.25.128.122/cae/0/". This portion is configurable based on the CdsOrigMgr NAS XML mounting file.
- $output_dir – "output"; This portion is configurable using either CLI or CDSM.
- $YYYY_MM_DD – "2012_04_05"
- $SE_hostname – "p-cae"
- $url_domain – "sjst81.cisco.com"
- $path – "sample"
- $asset_descriptor – "6d2f80bc00201109081355020052162f"
- $device_class – "iPhone4"
- $Adaptation_Profile_Index– "0"
- $container_type – "mp4"

Similarly, only the master (parent) manifest file is named using the above scheme for HLS ABR. The files for newly created ABR rate are named as follows:

- $new_rate_dir – "hls_rate_150000", where 150000 indicates its corresponding bit rate. This rate directory is located is the same directory as the parent manifest file.
- The child manifest file and its corresponding transcoded chunk (.ts) files are placed in the $new_rate_dir.

NAS Eviction

Both original and transcoded files are saved to NAS. The goal of NAS eviction is to ensure that there is always room on the NAS for new input or output files. When multiple OFAMs are deployed in the network, each OFAM performs its NAS eviction independently without causing conflict with others. This is because each OFAM only evicts the entries or files that it creates.

For HLS ABR, eviction is applied both to the parent manifest and to its child manifest and its chunk (.ts) files.

Input Files

In theory, input files are no longer needed after transcoding is completed, and so could be deleted immediately. However, it is sometimes helpful as a debugging aid to retain input files for a fixed time period after transcoding. Accordingly, input files and their associated directories are kept for up to two days before being evicted.

Note When NAS eviction occurs, the corresponding alarms are generated and then canceled.

Output Files

Eviction (deletion) of output files is efficiently managed by the AIM process because the AIM normally has a database entry for each transcoded asset. When multiple AIMs are deployed in an OE solution, each AIM should only evict the files (database entries) that are created by the same host. The creating hostname is embedded in the NAS directory. An empty NAS directory is deleted as it no longer contains any files.

Note NAS eviction works independently of AIM redundancy.

The AIM employs several mechanisms to decide to delete an output file:

Content Expiry

When a transcoded video file expires and is detected by the AIM as it scans through its database entries, the AIM deletes the database entry and its corresponding NAS file(s).

Triggers

Different mechanisms can trigger the eviction process. For example:

- The AIM periodically wakes up to check whether NAS utilization has reached a configured high watermark (default to 75%).
- Eviction is suspended once the low watermark of NAS utilization (default to 65%) is achieved.

Algorithm

The eviction algorithm is driven by the following parameters:

- **Last Access Time**. The AIM database tracks the Last Access Time for each asset and deletes the database entry and its NAS file starting with those with the oldest last access time.

  Note This field is synchronized among the AIMs if redundancy is enabled.

- **Dangling NAS Files**. A dangling NAS file is one that no longer has a corresponding AIM database entry. Dangling NAS files can be deleted at any time. To save resources, the AIM scans from the oldest directory forward to find dangling NAS files. Due to the distributed nature of the OE solution, it is possible for AIMs to delete too many files during NAS eviction. This requires the AIM to verify the low watermark after each small batch of files is deleted and stop eviction immediately once the low watermark is reached.
- **Two Phase Deletion**. In a distributed cluster, there is a delay for the database to synchronize among its nodes. To account for this, files to be deleted are marked for deletion in the first phase, or scan. The database entries and corresponding NAS files will be removed at a later AIM scan time.

Monitoring

KPI Reporting

The OE reports key performance indicators (KPIs) for its own features through the CDSM. The OE also reports KPIs on behalf of the CTM.

The OE and the CTM encoders generate reports indicating CPU loading, time taken to process content types, efficiencies gained by using the various techniques, average hold times for transformed content, storage status, and related parameters.

The OE is able to collect reports per website, per MVG, per VDS ingest point from the perspective of the OE, Per Device Class Transformation, Per Profile, Per Codec Type, and Per Container Type.

KPI reporting is configurable for the counters and the time interval, and supports the transfer of bulk statistics file to the CDSM via SFTP, FTP, or other required means. CTM encoders also report their KPIs through the OE.

Statistics Reporting

The CMS agent that resides on the device periodically collects statistics from the AIM, Web Engine, and other related processes, and sends these data to the CDSM. The user can request a statistics update by clicking **Update Statistics** on the CDSM toolbar. If the OE is disabled or if the process is not running, the value of statistical items will be **N/A** in the GUI page.

The OE provides a history of statistics per month, week, day, hour, and minute, including interaction logs with CDS, MVG, and the device database. This information helps operators predict the need for capacity expansion and provides them with advance notice of potential OE overload events.

The OE supports the generation of bulk statistics file in a specified format, which is currently used by the CDSM.

Note Clients that generate multiple range requests for a single video with different URLs will cause the popularity count for the video to be incremented multiple times, thereby inflating the popularity statistics for the video asset.

OFAM Statistics

Following is a complete sample list of statistics that the OFAM displays in response to the **show cae offline-mgr statistics** CLI command.

```
OFAM#show cae offline-mgr statistics

Offline-Mgr Progressive Statistics
    CAREQ Requests Recv                  :               5
    CAIND Response Sent                  :               5
    CANOT Response Sent                  :               0
    Fetch Requests Sent                  :               5
    Fetch Response Recv                  :               5
    Transcode Job Requests               :               4
    Transcode Job Response               :               4
    CAREQ Requests Recv failed           :               0
    CAIND Response Sent failed           :               0
    CANOT Response Sent failed           :               0
    Fetch Requests Sent failed           :               0
    Fetch Response Recv failed           :               0
    Cache-only success                   :               1
    Cache-only failed                    :               0
    Transcode Job Requests failed        :               0
    Transcode Job Response failed        :               0

Offline-Mgr HLS ABR Statistics
    Manifest CAREQ Requests Recv         :               0
    Manifest CAIND Response Sent         :               0
    Manifest CANOT Response Sent         :               0
    Manifest Fetch Requests Sent         :               0
    Manifest Fetch Response Recv         :               0
    Chunk Fetch Requests Sent            :               0
    Chunk Fetch Response Recv            :               0
    Chunk Transcode Job Requests         :               0
    Chunk Transcode Job Response         :               0
    Manifest CAREQ Requests Recv failed  :               0
    Manifest CAIND Response Sent failed  :               0
    Manifest CANOT Response Sent failed  :               0
    Manifest Fetch Requests Sent failed  :               0
    Manifest Fetch Response Recv failed  :               0
    Chunk Fetch Requests Sent failed     :               0
    Chunk Fetch Response Recv failed     :               0
    Chunk Transcode Job Requests failed  :               0
    Chunk Transcode Job Response failed  :               0
```

SE Statistics

Following is a complete sample list of statistics that the SE displays in response to the **show stat web-engine** CLI command.

```
SE#show stat web-engine

HTTP Request Info Statistics
-----------------------
Num Lookups                    :                           2
Preposition Hit                :                           0
External Hit                   :                           1
Cache Hit                      :                           1
Cache Miss                     :                           0
Partial Cache Hit              :                           0
Cache Bypass                   :                           0
```

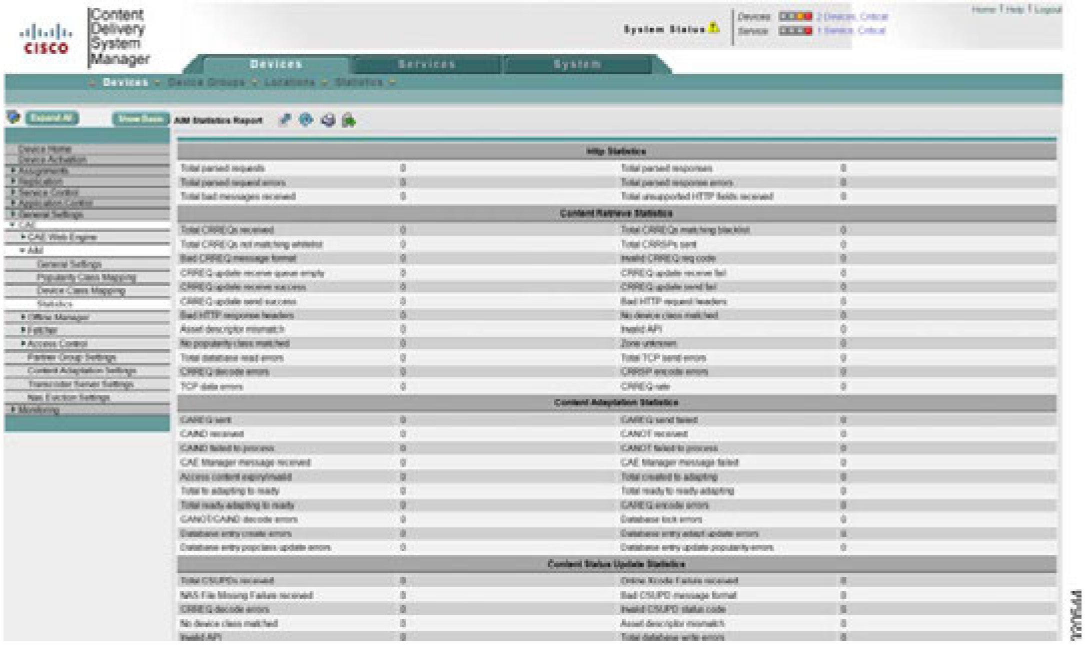
```
Live Miss                      :                           0
Live Hit                       :                           0
ASX Meta Response              :                           0

HTTP Request Type Statistics
-----------------------
Get Requests                   :                           2
Post Requests                  :                           0
Head Requests                  :                           0
Put Requests                   :                           0
Delete Requests                :                           0
Trace Requests                 :                           0
Options Requests               :                           0
Connect Requests               :                           0
Patch Requests                 :                           0
Unknown HTTP Method Requests   :                           0
Range Requests Received        :                           0
Range Requests Sent            :                           0
Revalidation Requests Received :                           0
Revalidation Requests Sent     :                           0
Liveness Query                 :                           0
CAE Liveliness Requests        :                           0
WMT(http) Redirected Requests  :                           0
Local Requests                 :                           0
Play Live Requests             :                           0
Total Outgoing Requests        :                           2

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

HTTP Performance Statistics
----------------------
Total Bytes In                 :                           0
Total Bytes Out                :                     7401002
Total Requests                 :                           2

Web-Engine CAE Statistics
----------------------
Transcoded Offline Content     :                           0
Transcoded Online Content      :                           0
Cache-Only Offline Content     :                           2
Redirected Request to SR       :                           0
Total Bytes Saved through Xcoding:                         0
Online Bytes Saved through Xcoding:                        0
Offline Bytes Saved through Xcoding:                       0
Total Bytes Saved through Caching (local):                   3700219
Total Bytes Saved through Caching (NAS mount):               3700219
Total Bytes Out Excluding Headers:                   7400438
Online Bytes Out Excluding Headers:                        0
Offline Bytes Out Excluding Headers:                 7400438
CAE Bypass Overall Content     :                           0
CAE Bypass Based on Response Headers:                      0
CAE Bypass Unsupported Query in URL:                       0
CAE Bypass Non-Video Content   :                           0
CAE Bypass Transcode Video Not-supported:                          0
CAE Bypass Transcode OFAM Error Code:                      0
CAE Bypass CRREQ Error         :                           0
CAE Bypass Internal Error      :                           0
CAE Bypass Due to Blacklist/Whitelist Match:                       0
CAE Bypass Online Transcode Setup Fail:                    0
CAE Bypass Online Transcode Template Not Found:                    0
Average Requests Per Second    :                        0.06
Average Bytes Per Second       :                   238742.00
Overall Ratio of Xcoded size/Actual size(Compression Ratio):    1.000000
Online Ratio of Xcoded size/Actual size(Compression Ratio):     1.000000
Offline Ratio of Xcoded size/Actual size(Compression Ratio):    1.000000
Statistics was last cleared on Tuesday, 30-Apr-2013 11:47:12 UTC.
```

Viewing AIM Statistics

To view statistics for the AIM, do the following:

Step 1 Choose **Devices > Devices > CAE > AIM > Statistics**. The AIM Statistics page is displayed.

Figure 4-1 AIM Statistics



Http Statistics			
Total parsed requests	0	Total parsed responses	0
Total parsed request errors	0	Total parsed response errors	0
Total bad messages received	0	Total unsupported HTTP fields received	0
Content Retrieve Statistics			
Total CRREQs received	0	Total CRREQs matching blacklist	0
Total CRREQs not matching whitelist	0	Total CRRSPs sent	0
Bad CRREQ message format	0	Invalid CRREQ req code	0
CRREQ update receive queue empty	0	CRREQ update receive fail	0
CRREQ update receive success	0	CRREQ update send fail	0
CRREQ update send success	0	Bad HTTP request headers	0
Bad HTTP response headers	0	No device class matched	0
Asset descriptor mismatch	0	Invalid API	0
No popularity class matched	0	Zone unknown	0
Total database read errors	0	Total TCP send errors	0
CRREQ decode errors	0	CRRSP encode errors	0
TCP data errors	0	CRREQ rate	0
Content Adaptation Statistics			
CAREQ sent	0	CAREQ send failed	0
CAIND received	0	CANOT received	0
CAIND failed to process	0	CANOT failed to process	0
CAE Manager message received	0	CAE Manager message failed	0
Access content expiry/invalid	0	Total created to adapting	0
Total to adapting to ready	0	Total ready to ready adapting	0
Total ready adapting to ready	0	CAREQ encode errors	0
CANOT/CAIND decode errors	0	Database lock errors	0
Database entry create errors	0	Database entry adapt update errors	0
Database entry popclass update errors	0	Database entry update popularity errors	0
Content Status Update Statistics			
Total CSUPDs received	0	Online Xcode Failure received	0
NAS File Missing Failure received	0	Bad CSUPD message format	0
CRREQ decode errors	0	Invalid CSUPD status code	0
No device class matched	0	Asset descriptor mismatch	0
Invalid API	0	Total database write errors	0

Step 2 On this page, view AIM statistics that are periodically collected from the system database by the CDSM.

Note To manually update the statistics display, click **Update Statistics** on the toolbar.

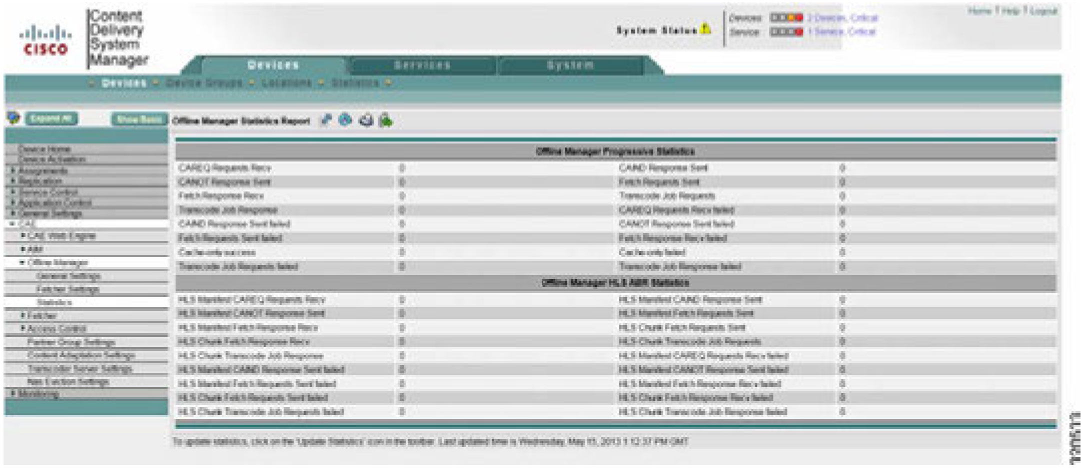
Note If OE is disabled or process is not running, the value of statistics items will be N/A.

Viewing Offline Manager Statistics

To view statistics for the OM, do the following:

Step 1 Choose **Devices > Devices > CAE > Offline Manager > Statistics**. The Offline Manager Statistics page is displayed.

Figure 4-2 Offline Manager Statistics



Offline Manager Statistics Report

Offline Manager Progressive Statistics			
CAREQ Requests Recv	0	CAND Response Sent	0
CANOT Response Sent	0	Fetch Requests Sent	0
Fetch Response Recv	0	Transcode Job Requests	0
Transcode Job Response	0	CAREQ Requests Recv failed	0
CAND Response Sent failed	0	CANOT Response Sent failed	0
Fetch Requests Sent failed	0	Fetch Response Recv failed	0
Cache-only success	0	Cache-only failed	0
Transcode Job Requests failed	0	Transcode Job Response failed	0
Offline Manager HLS ABR Statistics			
HLS Manifest CAREQ Requests Recv	0	HLS Manifest CAND Response Sent	0
HLS Manifest CANOT Response Sent	0	HLS Manifest Fetch Requests Sent	0
HLS Manifest Fetch Response Recv	0	HLS Chunk Fetch Requests Sent	0
HLS Chunk Fetch Response Recv	0	HLS Chunk Transcode Job Requests	0
HLS Chunk Transcode Job Response	0	HLS Manifest CAREQ Requests Recv failed	0
HLS Manifest CAND Response Sent failed	0	HLS Manifest CANOT Response Sent failed	0
HLS Manifest Fetch Requests Sent failed	0	HLS Manifest Fetch Response Recv failed	0
HLS Chunk Fetch Requests Sent failed	0	HLS Chunk Fetch Response Recv failed	0
HLS Chunk Transcode Job Requests failed	0	HLS Chunk Transcode Job Response failed	0

To update statistics, click on the 'Update Statistics' icon in the toolbar. Last updated time is Wednesday, May 15, 2013 1:12:37 PM GMT

Step 2 On this page, view OM statistics periodicaly collected by the CDSM from the system database.

Note You can manually update the statistics display by clicking **Update Statistics** on the toolbar.

Note If the OE is disabled or if the process is not running, the value of statistics items will be N/A.

Statistics for 3GP and 3G2 Video

Two OFAM counters, Cache-only Success and Cache-only Fail, indicate how many 3GP and 3G2 videos crossed the popularity threshold and attempted cache-only optimization. The Success counter indicates how many were successfully cached, while the Failed counter indicates how many failed. The sum of these two counters indicates how many videos attempted local caching.

Example

```
OFAM#show cae offline-mgr statistics
. . .
Offline-Mgr Progressive Statistics
----------------------
    . . .
    Cache-only success                  :             10
    Cache-only failed                   :               0
    . . .
```

In addition, the following statistics on the SE indicate how many requests served by the SE account for the videos which were Cache-Only.

Example

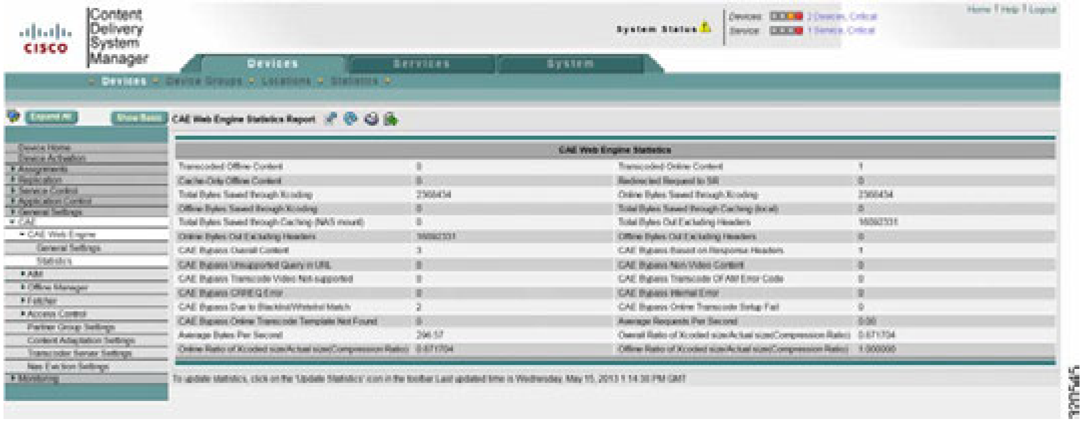
```
SE#show statistics web-engine
. . .
Web-Engine CAE Statistics
----------------------
Transcoded Offline Content     :                          0
Transcoded Online Content      :                         0
Cache-Only Offline Content     :                          10
. . .
```

Viewing Web Engine Statistics

To view statistics for the Web Engine, do the following:

Step 1 Choose **Devices > Devices > CAE > CAE Web Engine > Statistics**. The Web Engine Statistics page is displayed.

Figure 4-3 Web Engine Statistics



CAE Web Engine Statistics Report

CAE Web Engine Statistics			
Transcoded Offline Content	0	Transcoded Online Content	1
Cache-Only Offline Content	0	Redirected Request to SR	0
Total Bytes Saved through Xcoding	2360434	Online Bytes Saved through Xcoding	2360434
Offline Bytes Saved through Xcoding	0	Total Bytes Saved through Caching (local)	0
Total Bytes Saved through Caching (NAS mount)	0	Total Bytes Out Excluding Headers	16092331
Online Bytes Out Excluding Headers	16092331	Offline Bytes Out Excluding Headers	0
CAE Bypass Overall Content	3	CAE Bypass Based on Response Headers	1
CAE Bypass Unsupported Query in URL	0	CAE Bypass Non Video Content	0
CAE Bypass Transcode Video Not supported	0	CAE Bypass Transcode Of AM Error Code	0
CAE Bypass ORREQ Error	0	CAE Bypass Internal Error	0
CAE Bypass Due to Blacklist/Whitelist Match	2	CAE Bypass Online Transcode Setup Fail	0
CAE Bypass Online Transcode Template Not Found	0	Average Requests Per Second	0.00
Average Bytes Per Second	296.57	Overall Ratio of Xcoded size/Actual size(Compression Ratio)	0.671704
Online Ratio of Xcoded size/Actual size(Compression Ratio)	0.671704	Offline Ratio of Xcoded size/Actual size(Compression Ratio)	1.000000

To update statistics, click on the 'Update Statistics' icon in the toolbar. Last updated time is Wednesday, May 15, 2013 1:14:30 PM GMT

Step 2 On this page, view Web Engine statistics that the CDSM periodically collects from the system database.

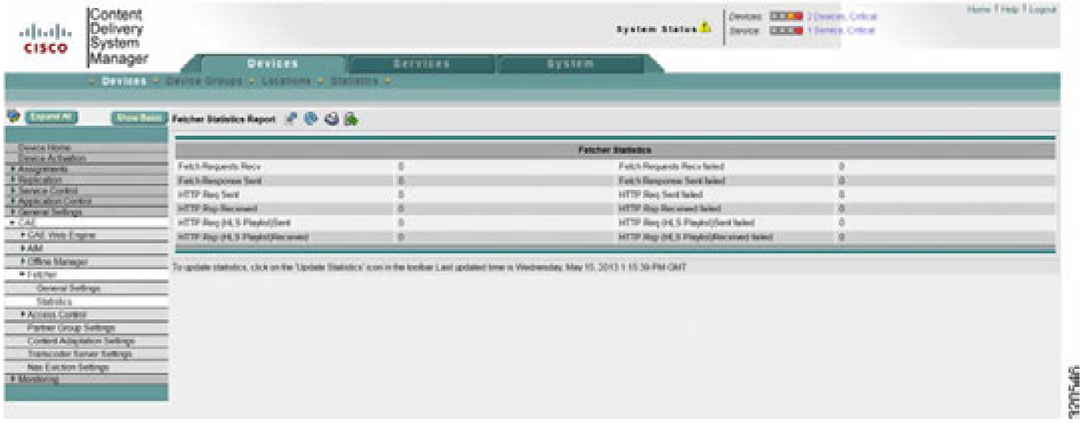
Note You can manually update statistics by clicking **Update Statistics** on the toolbar.

Viewing Fetcher Statistics

To view statistics for the Fetcher, do the following:

Step 1 Choose **Devices > Devices > CAE > Fetcher > Statistics**. The Fetcher Statistics page is displayed.

Figure 4-4 Fetcher Statistics



Fetcher Statistics			
Fetch Requests Recv	0	Fetch Requests Recv failed	0
Fetch Response Sent	0	Fetch Response Sent failed	0
HTTP Req Sent	0	HTTP Req Sent failed	0
HTTP Rsp Received	0	HTTP Rsp Received failed	0
HTTP Req (HLS Playlist)Sent	0	HTTP Req (HLS Playlist)Sent failed	0
HTTP Rsp (HLS Playlist)Received	0	HTTP Rsp (HLS Playlist)Received failed	0

To update statistics, click on the 'Update Statistics' icon in the toolbar. Last updated time is Wednesday, May 15, 2013 1:15:39 PM GMT

Step 2 On this page, view Fetcher statistics that CDSM periodically collects from the system database.

Note You can manually update statistics by clicking **Update Statistics** on the toolbar.

Note If the OE is disabled or if the OE process is not running, the value of the statistics items will be N/A.

Video Transaction Logs

A Transaction Log is generated for each video served. Transaction Logs are written directly to the CAE-SE file system as flat text files. The general output format of each Transaction Log is defined as follows:

```
{CTM Encoder IP Address} | {CTM Encoder Port} | {JobID} | {FlowID} | {template id} | {Job
Status Code} | {Encoder Status Code} | {Bytes sent to encoder} | {Bytes received from
encoder} | {Resolution width override} | {Resolution height override} {Bit rate override}
| {Compression override} | {Min Bit Rate Override} | {Min Frame Rate Override} | {Frame
Rate Reduction Override}
```

For Example:

```
172.25.100.61|8005|3500|-595007873|242|ok|EncodeComplete|129056926|124085521|0|0|0|60|
250000|0|1
```

Custom Transaction Log Tokens

The following table describes the tokens that are used to define the format of custom OE transaction logs. The tokens listed first in the table are taken from VDS-IS. Later tokens with the prefix [CAE] are specific to the OE.

Table 4-1 Transaction Log Tokens

Token	Description
%a	IP address of the requesting client
%A	P address of the CAE-SE
%b	Bytes sent, excluding HTTP headers
%C	ThinkTimes – Time to Auth | Time to Lookup | Time to Route | Time to OS ? (ms)
%D	Time consumed to serve the request in microseconds
%h	Remote host (IP address of the requesting client is logged)
%H	Request protocol
%I	Bytes received from the client
%g	Storage URL
%G	Source URL
%m	Request method
%O	Bytes sent to client, including the headers
%q	Query string (which is preceded by a question mark (?) if a query string exists; otherwise, it is an empty string)
%r	First line of the request
%Z	Request receive time (formatted)
%>s	Status; the transaction log code always returns the HTTP response code for the request
%t	Time in common log time format (or standard English format)
%T	Time consumed to serve the request in seconds (a floating point number with 3 decimal places)
%u	URL path requested, 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.
%X	Connection status when the response is completed
%M	Mime Type
%L	Asset Size
%I	Bytes Requested + Response Header Length
%J	NetworkXferAvgRtt | NetworkXferMaxRtt
%K	NetworkXferCwndFlicker
%N	NetworkXferIfName
%{<header_name>}i	HTTP Header as specified by header name; can be standard or non-standard headers; one entry for each header. For example, %{User-Agent }i.

Token	Description
%[CAE]s	Client Serving Type and (optional) Bypass Reason. Possible values for Client Serving Type: OFFLINE_XCODED_NAS_MOUNT OFFLINE_XCODED_NAS_HTTP OFFLINE_XCODED_LOCAL_CACHE ONLINE_XCODED ONLINE_VIDEO_BYPASS ONLINE_NONVIDEO_BYPASS OFFLINE_SR_REDIRECT ONLINE_ABR_PARENT_MANIFEST ONLINE_ABR_CHILD_MANIFEST OFFLINE_ABR_CHILD_MANIFEST Possible values for Bypass Reason: ExistDataSourceNotFoundFor RangeRequest UnsupportedMediaFormat UnknownMediaFormat MetaDataAbsertForH264FLV UnsupportedURLParameters ResponseHeaderNotOK TranscodeNotSupported NonVideoContent FailedToPostJobToArmada UnableToFindTemplate ErrorReceivedFromOFAM Unknown
%[CAE]t	Bytes saved due to transcoding; that is, the difference between the bytes that would have been served to the client and the actual bytes served
%[CAE]x	Compression ratio (bytes actually served to client) / (bytes that would be served from OS). This is for both online or offline transcoding
%[CAE]c	Bytes saved due to caching; that is, the bytes that would have been retrieved directly from the OS if not for caching; either local or NAS
%[CAE]d	Device Class
%[CAE]p	Popularity Class
%[CAE]a	Asset Descriptor
%[CAE]i	API (Adaptation Profile Index)
%[CAE]o	Online Transcoding Attributes
%[CAE]b	Bit-rate Indication

The following is an example of a custom Transaction Log format using these tokens.

```
transaction-logs format custom "%U %O %b %I %m %>s %R %H %{User-Agent}i %{Host}i
%{X-adaptation-profile-index}i %{X-forwarded-dest-addr-port}i %{Range}i %{Last-Modified}o
%{Content-Type}o %{ETag}o %[CAE]x %[CAE]d %[CAE]p %[CAE]i %[CAE]t %[CAE]s %[CAE]c %[CAE]a
%[CAE]o"
```

Transaction Logs for 3GP and 3G2 Video

The transaction logs captured on the SE carry the following tags for the client-serving type when serving cached 3GP and 3G2 videos:

- OFFLINE_CACHE_ONLY_NAS_MOUNT: When the video is served from the NAS.
- OFFLINE_CACHE_ONLY_LOCAL_CACHE: When the video is served from SE local cache.
- ONLINE_VIDEO_BYPASS|UnsupportedMediaFormat: The SE continues to use the bypass tag as the client serving type for 3GP and 3G2 video that has not crossed the popularity threshold, or for videos that have crossed the threshold but are currently unavailable for offline serving.

For example:

```
[18/Apr/2013:13:43:54+0000] http://172.25.128.81/3gp-videos/paint.3gp 1147127 GET 200
TCP_HIT_ABORTED HTTP/1.1
172.25.128.81 video/3gpp - 1 BigScreenDevice 0 OFFLINE_CACHE_ONLY_NAS_MOUNT
e93d0c560020130416141753003875fb
54000|54000 176|144|12|364|mp4v - Mozilla/5.0 (iPad; CPU OS 6_1_2 like Mac OS X)
AppleWebKit/536.26 (KHTML, like Gecko)
Version/6.0 Mobile/10B146 Safari/8536.25
[18/Apr/2013:13:43:55+0000] http://172.25.128.81/3gp-videos/paint.3gp 354 GET 206 TCP_HIT
HTTP/1.1 172.25.128.81
video/3gpp bytes=0-1 1 BigScreenDevice 0 OFFLINE_CACHE_ONLY_LOCAL_CACHE
e93d0c560020130416141753003875fb
54000|54000 176|144|12|364|mp4v - AppleCoreMedia/1.0.0.10B146 (iPad; U; CPU OS 6_1_2 like
Mac OS X; en_us)
[30/Apr/2013:10:51:48+0000] http://172.25.128.81/3gp-videos/paint.3gp 3700501 GET 200
TCP_MISS HTTP/1.1172.25.128.81
video/3gpp - 1 BigScreenDevice 0 ONLINE_VIDEO_BYPASS|UnsupportedMediaFormat
e93d0c560020130416141753003875fb
54000|54000 176|144|12|364|mp4v - Wget/1.10.2 (Red Hat modified)
```

SNMP MIBs and Alarms

The OE uses SNMP Management information bases (MIBs) to gather statistics and perform other reporting and alarm functions. SNMP MIBs are defined to support traps for the OE-VDS interface, OE-MVS interface, and OE internal video components. The OE and its interface functions have configurable logic to allow for sending traps when a defined condition is reached.

The OE also supports SNMP MIBs for gathering KPIs for video performance. The Transcoder encode nodes support SNMP MIBs and traps via the OE. The counter group “cdsCaeGroup” accommodate the following counters:

- CRREQ sent
- CRREQ recv
- CRRSP sent
- CRRSP recv (not in cache/nas)
- CRRSP recv (in cache/nas)

- CAREQ sent
- CAREQ recv
- CAIND sent
- CAIND recv
- CANOT sent
- CANOT recv

As a part of health monitoring, the Offline Manager is responsible for watching NAS disk usage, and issues the following alarms in response:

- **Critical Alarm**. Indicates that the NAS device is not reachable.
- **Major Alarm**. Indicates that NAS disk usage has exceeded a threshold. CPU and memory currently exists in the Web Engine.

In addition, the OE monitors communications with the OFAM, and issues the following alarms in response:

- **Critical Alarm**. Indicates that the Transcoder adaptation template is not reachable for the CAE-OFAM.
- **Major Alarm**. Indicates that occurs when the MasterDB in CDSM is not reachable for CAE-OFAM.

CHAPTER 5

Troubleshooting the VDS-OE

Overview

This chapter provides information on VDS-OE troubleshooting.

OFAM Troubleshooting

This section describes troubleshooting steps for the AIM, OM, and Fetcher components of the OFAM.

General Checklist

1. You should be able to ping configured IP address of the transcoder server:

```
#ping configured-transcoder-IP
```

2. Make sure that OFAM processed are running:

```
#show aim statiscics
#show cae offline-mgr statistics
#show cae fetcher statistics
```

3. If the above CLI is disabled, make sure that the following CLI is configured:

```
#cae ofam-mode enable
```

4. Make sure that the connections from Web Engine (client) are established:

```
#show aim connections client
```

5. If there is no connection from a remote Web Engine (i.e., it is IP is not 127.0.0.1), go to the intended CAE SE to configure its AIM IP addresses.
6. Make sure that NAS is properly mounted on the OFAM:

```
#show content-origin
```

The Status field should display **Success**.

7. Make sure that the default adaptation file **factory.xml** is loaded properly:

```
#show cae adaptation device
```

The output lines should show their template id is not equal to -1(usually, they are id=4xx or id=5xx).

AIM Troubleshooting

Check for Normal Operation

Use the following commands to check for normal AIM operation:

1. To check the total number of AIM entries:

   ```
   show aim database summary
   ```

2. To check the detail entry status:

   ```
   show aim database all
   ```

3. To check all statistics:

   ```
   show aim statistics all
   ```

4. To check for a coredump alarm (report any such alarm to Cisco):

   ```
   show alarm
   ```

5. To check for logged errors (report any such alarms to Cisco):

   ```
   tail aim logs
   ```

6. To check CAE adaptation:

   ```
   show cae adaptation all
   ```

OM Troubleshooting

The following CLI commands can be helpful in debugging:

```
#show cae offline-mgr statistics
#show cae offline-mgr session all
#show cae offline-mgr session asset-descriptor
```

Fetcher Troubleshooting

If the Fetcher fails, do the following:

```
#show cae fetcher statistics
#show cae fetcher session all
```

Step 1 Check to see if the OFAM SE can ping the origin server to confirm that the server is reachable.

Step 2 Check to see if the NAS is mounted. You can view the status of NAS mount by reading the **/etc/NASinfo** file.

Step 3 Check to see if the NAS mount directory is writable from the OFAM SE.

Step 4 Confirm that the Fetcher is listening on the correct port and that the connection between the Offline Manager and Fetcher are in the “established” state.

Step 5 Check Fetcher statistics using the CLI command **show cae fetcher statistics**.

Encode Node Troubleshooting

For information on encode node troubleshooting, see the *Cisco Transcode Manager User Guide v4.5 (78-20395-01)*.

NAS Replacement

When replacing a NAS, it is necessary to remove the AIM entries for the NAS that is being replaced. There are two possible scenarios for doing this:

- Remove all AIM entries immediately when notified of the NAS mount change.
- Remove the AIM entry only when the corresponding video asset is next requested and found to be unreachable.

APPENDIX A

Sample Configurations

Sample SE Configuration

Note VDS-OE Release 1.0 supports video analysis of MP4 and FLV content only. For other content types, such as WMV and MOV, the bit rate and frame rate default to zero and cannot be configured in the XML file.

```
p-cae#sh run
! CAE version 2.6.1
!
device mode service-engine
!
!
hostname p-cae
!
!
!
!
!
!
ip domain-name cisco.com

interface GigabitEthernet 1/0
ip address 172.25.128.43 255.255.255.0
mtu 1470
exit
interface GigabitEthernet 2/0
mtu 1470
shutdown
exit
!

streaming-interface GigabitEthernet 2/0

ip default-gateway 172.25.128.1
!
!
primary-interface GigabitEthernet 1/0
!
transaction-logs enable
transaction-logs export interval every-hour at 13
transaction-logs export ftp-server 172.25.128.44 admin **** /translogs/export
transaction-logs format custom "%t %U %O %m %>s %R %H %{Host}i %{Content-Type}o %[CAE]x
%[CAE]d %[CAE]i %[CAE]s %[CAE]a
```

```
%[CAE]b %[CAE]v %[CAE]o %{User-Agent}i"
!
!
!
!
!
ip name-server 171.70.168.183
ip name-server 171.68.226.120
!
!
!
logging console enable

cdsm ip 172.25.128.44
cms enable
!
!
!
!
!
!
cae enable
cae xcode server ip 172.25.128.152 port 8062
cae web-engine aim primary-ip 172.25.128.57 port 8001
cae web-engine aim secondary 172.25.128.58
```

Sample OFAM Configuration

```
! CAE version 2.6.1
!
device mode service-engine
!
!
hostname p-cae
!
!
!
!
!
!
ip domain-name cisco.com
!
!
!
!
!
!
interface GigabitEthernet 1/0
ip address 172.25.128.43 255.255.255.0
mtu 1470
exit
interface GigabitEthernet 2/0
mtu 1470
shutdown
exit
!
streaming-interface GigabitEthernet 2/0
!
!
ip default-gateway 172.25.128.1
!
```

```
!
primary-interface GigabitEthernet 1/0
!
!
!
!
!
ip name-server 171.70.168.183
ip name-server 171.68.226.120
!
!
!
logging console enable
!
cae enable
cae ofam-mode enable
cae xcode server ip 172.25.128.152 port 8062
cae adaptation-rule file /state/contentAdptFiles/factory.xml

cae source-content-group blacklist 56.com
match referrer "56img.com"
match http-header Server "Tengine"
match http-header Content-Type "flv"
exit
!

cae source-content-group blacklist youku.com
match user-agent "Lavf"
match http-header Server "YOUKU"
match http-header Content-Type "flv"
exit
!
aim asset-manager
device-class SmallScreenDevice
priority 2
match http user-agent .*HD7.*
match http user-agent .*HTC.*
match http user-agent .*MOT-ME811.*
match http user-agent .*Nexus.S.4G.*
match http user-agent .*Nokia.*
match http user-agent .*SGH.*
match http user-agent .*iPhone.*
match http user-agent .*Windows\s*Phone.*
exit
!
device-class BigScreenDevice
priority 1
match http user-agent .*Chrome.*
match http user-agent .*Firefox.*
match http user-agent .*GT-P7500.*
match http user-agent .*iPad.*
match http user-agent .*Kindle.Fire.*
match http user-agent .*MSIE.*
match http user-agent .*Macintosh.*
match http user-agent .*Moz.*
match http user-agent .*Red.*
match http user-agent .*Tablet.*
match http user-agent .*Windows.*
exit
!
device-class AnyDevice
priority 0
match http user-agent .*
exit
```

```
!
popularity-class AnyDevice
priority 0
threshold one-day 2
match-rule user-agent .*
exit
!
exit
!
no authsvr enable
```

Sample MVG Configuration

```
cae-group lab
      local-addr 10.75.173.245
      server se77 addr 10.74.31.77 port 80
      server se78 addr 10.74.31.78 port 80
      server se72 addr 10.74.31.72 port 80
      keepalive-server interval 10 num-retry 3 timeout 3 deadtime 120 port 80
   #exit
#exit
```

Sample Adaptation XML File

```
<?xml version="1.0" encoding="UTF-8"?>
<CAEGlobalConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="CAEGlobalConfig.xsd">
  <Revision>1.0</Revision>
  <CustomerName>TBD</CustomerName>
  <Rule_Patterns>

    <DeviceClass id=”iPhone”>
      <Template> cae-template-iPhone-h264 </Template>
      <Template> cae-template-iPhone-vp6 </Template>
    </DeviceClass>

    <DeviceClass id=”iPad”>
      <Template> cae-template-iPad-h264 </Template>
      <Template> cae-template-iPad-vp6 </Template>
    </DeviceClass>

    <DeviceClass id=”galaxy”>
      <Template> cae-template-galaxy-h264 </Template>
      <Template> cae-template-galaxy-vp6 </Template>
    </DeviceClass>


    <PatternListGrp id="Apple_API_0">
      <DeviceClass>iPhone</DeviceClass>  <!—either iPhone or iPad -->
      <DeviceClass>iPad</DeviceClass>
      <AdapatationProfileIdx>0</AdapatationProfileIdx>
      <InputVideoRateStartEnd>500000-2000000 </InputVideoRateStartEnd>
      <InputVideoFrameRateStartEnd>20-50</InputVideoFrameRateStartEnd>
      <MatchedParnterGrp>gold-partner</MatchedParnterGrp>
      <!--<AccessNetwork>3g</AccessNetwork>-->
      <ContentSourceType>mp4</ContentSourceType>
    </PatternListGrp>
    <PatternListGrp id="iPhone_API_3">
      <DeviceClass>iPhone</DeviceClass>
      <AdapatationProfileIdx>0</AdapatationProfileIdx>
    </PatternListGrp>

    <PatternListGrp id="Samsung_API_3">
      <DeviceClass>Galaxy</DeviceClass>
      <AdapatationProfileIdx>0</AdapatationProfileIdx>
    </PatternListGrp>

  </Rule_Patterns>

  <Rule_Actions>
    <Rule_SetAction name="BasicUserService">
      <SetParameter  name="Progressive-Video">
        <MaxCompressionRatio>50</MaxCompressionRatio>
        <Resolution>320x240</Resolution>
        <MinBitRate>200000</MinBitRate>
        <OutputBitRate>300000</OutputBitRate>
        <OutputFrameRate>15</OutputFrameRate>
        <Pacing>0</Pacing>
      </SetParameter>

      <SetParameter  name="ABR-Rate-Delete">
        <StartEnd>2000000-4000000</StartEnd>
        <StartEnd>800000-160000</StartEnd>
      </SetParameter>

      <SetParameter  name="ABR-Rate-Insert">
        <StartEnd>100000-200000</StartEnd>
        <InsertRate>150000</InsertRate>
      </SetParameter>
    </Rule_SetAction>

  <Rule_SetAction name=”Silver-User-Action>
     <SetParameter  name="Progressive-Video">
      <MaxCompressionRatio>40</MaxCompressionRatio>
      <MinBitRate>240000</MinBitRate>
      <OutputBitRate>320000</OutputBitRate>
      <Pacing>0</Pacing>
     </SetParameter>

     <SetParameter  name="ABR-Rate-Delete">
       <StartEnd>2000000-4000000</StartEnd>
       <StartEnd>800000-160000</StartEnd>
     </SetParameter>

     <SetParameter  name="ABR-Rate-Insert">
       <StartEnd>200000-300000</StartEnd>
       <InsertRate>250000</InsertRate>
     </SetParameter>
   </Rule_SetAction>


   <PatternList_Action_Map>
     <SetParameter matchGroup="Apple_API_0">
       <Action>Basic-User-Action </Action>
     </SetParameter>

     <SetParameter matchGroup="iPhone_API_3">
       <Action>Silver-User-Action </Action>
     </SetParameter>

     <SetParameter matchGroup="Samsung_API_3">
```

```
       <Action>Silver-User-Action </Action>
     </SetParameter>
   </PatternList_Action_Map>

  </Rule_Actions>

</CAEGlobalConfig>
```

APPENDIX B

CLI Commands

Global Configuration

Global configurations are downloaded to CAE nodes from CDSM through a device group. After downloading, the commands are wrapped in XML file format and transported to the CAE cluster using the HTTPS protocol.

Enable/Disable CAE

CAE capability is enabled by default, but can be disabled globally, that is, for all CAE nodes.

Syntax

Use this command to enable CAE capability on this node:

```
cae enable
```

Use the **no** form of this command to disable CAE on this node:

```
no cae enable
```

Enable/Disable CAE OFAM Mode

Use the following CLI commands to control all OFAM processes when in CAE-SE mode.

Syntax

Use this command to restrain all OFAM processes when in CAE-SE mode.

```
cae ofam-mode enable
```

Note You can only enter this command if **cae enable** is configured. Once configured, it will launch the OFAM (AIM, Offline Manager, and Fetcher) processes.

Use the no form of this command to stop the OFAM (AIM, Offline Manager, and Fetcher) processes.

```
no cae ofam-mode enable
```

Use this command to enable the CAE feature.

```
cae enable
```

Note This command launches the OFAM processses only if **cae ofam-mode enable** is configured.

Use the **no** form of this command to disable CAE processes, including OFAM processes.

```
no cae enable
```

Enable/Disable OFAM

The OFAM mode or service is not enabled by default, but you can enable it through the CLI.

Syntax

Use this command to enable OFAM capability for the node:

```
cae ofam-mode enable
```

Use the **no** form of this command to disable OFAM for the node:

```
no cae ofam-mode enable
```

Note These commands can be entered only if "cae enable" is configured.

Transcoder Server IP Address

WebEngine and Offline Manager both communicate with the Transcoder server to submit transcoding jobs. To establish communication with the Transcoder server, its IP address must be specified in advance.

Use the following command to allow WebEngine or Offline Manager to specify the Transcoder server IP address so it can communicate with the Transcoder server.

```
cae xcode server ip <x.x.x.x> port <port_number>
```

where <x.x.x.x> is the server IP address and <port_number> is the port number of the Transcoder server.

Note The default port number for the Transcoder server is 8062.

NAS Eviction

Use these commands to set the frequency and high and low trigger thresholds (“water marks”) for NAS eviction.

```
cae nas eviction frequency 2 // default to every 2 hours
cae nas eviction high-water-mark 75
cae nas eviction low-water-mark 65
```

Note All of these commands have corresponding controls in the CDSM GUI.

IP Address Range

The Transparent Proxy feature requires that a range of IP address be configured for every CAE card. Use the following commands to configure an IP address range for each card.

IP Interface

Use this command to specify the CAE card that is to receive the subsequent CLI command.

```
cds(config)#interface <port_type> <chassis/slot>
```

Where <port_type> is the port used to communicate with the card <chassis/slot> is the chassis and slot number of the CAE card to be configured.

IP Address Range

Use this command to specify the IP address range and subnet mask for the CAE card to be configured.

```
cds(config-if)#ip address range <ip_address_start> <ip_address_end> <subnet_mask>
```

Where <ip_address_start>, <ip_address_end>, and <subnet_mask> are the starting address, ending address, and IP subnet mask for the card, respectively.

Example

In the following example, the CAE card in chassis 1, slot 0 is specified for communication via its Gigabit Ethernet port. Then, the card is configured with IP address range 172.25.128.45 through 49 and subnet mask 255.255.0.0.

```
cds(config)#interface GigabitEthernet 1/0
cds(config-if)#ip address range 172.25.128.45 172.25.128.49 255.255.0.0
```

Adaptation Configuration

The objective of an adaptation configuration is to define the transcoding, ABR manifest file manipulation, and pacing actions that are needed for a particular input video or manifest file.

The adaptation configuration is used for both online and offline transcoding. It is used by WebEngine for online transcoding, and by CAE Offline Manager for offline transcoding.

Note We do not recommend changing the adaptation configuration through the CLI, as the XML file is downloaded from CDSM.

Content Source Group

A content source group defines the business partners for the service provider so that different adaptation policies can be applied for different business partners. Use the following command to define a content source group.

```
cae content-source-group gold-partner
  domain www.youtube.com     // match any of them
  domain www.netflix.com
  domain www.cnn.com
```

```
exit

cae content-source-group silver-partner
  domain www.cbs.com
exit

cae content-source-group any       // empty as default
exit
```

Global Exec CLI

The CLI commands described in this section run in execute mode rather than config mode.

Backup/Restore VDS-OE Database

Use this command to regularly back up the VDS-OE database and to restore it when necessary. This command is executed in the CDSM device.

```
cae database backup // back up to local default path
cae database restore <restore_file> // restores the file from the local default path
cae database ftp backup <ftp_ip> <ftp_user> <ftp_pw> <ftp_path>
cae database ftp restore <ftp_ip> <ftp_user> <ftp_pw> <ftp_path> <restore_file>
```

Where <restore_file> is the dump file generated by the backup operation; and where <ftp_ip>, <ftp_user>, <ftp_pw>, <ftp_path>, and <subnet_mask> are the FTP server IP address, user name, password, and file path for the restore file, respectively.

Example

The following examples show a backup and subsequent restore operation for the file named ftp_backup-2013-03-05-00-55-28.gz located at IP address 10.74.23.152.

```
cdsm#cae_database_ftp_backup 10.74.23.152 ftp ftp /var/ftp
cdsm#cae_database_ftp_restore 10.74.23.152 ftp ftp /var/ftp backup-2013-03-05-00-55-28.gz
```

AIM CLI

All AIM CLI commands must also be made available in CDSM. AIM functionality is enabled when CAE is enabled.

AIM Configuration

AIM TCP port

Use the AIM TCP port command to configure a non-default port to which the clients of AIM will connect.

Note The default port number for AIM TCP is 8001.

Syntax

```
aim tcp port <port-number>
```

Use the **no** form of the command to delete a non-default AIM TCP port. The following example shows such a deletion.

```
no aim tcp port <port-number>
```

Device Class

Use the Device Class command to map HTTP headers to a device class, or to remove such a mapping if already defined.

Syntax

```
aim asset-manager
    device-class <class-name>
        match http { <user-agent> | <host> | <uribase> | <param> | header
<header-name>}  <reg-exp-string>
        priority <num:0-255>
```

The following table describes the parameters used in this command.

Syntax Description

class_name	Class name string.
user-agent	User-agent in the HTTP header. The value can be specified either in normal string or reg-exp string format.
host	Host in HTTP header. The value can be specified either in normal string or reg-exp string format.
uribase	The uribase from Request-URI.
param	Parameters in Request_URI, such as ID, format, etc. The value can be specified either in normal string or reg-exp string format. For example, “.*(id=.+)\&”, or “.*(key=.+)\&” will match and collect “id=e8996ff05f5c” and “key=ytal” from Request-URI.
header	You can specify any other header in HTTP GET/POST messages.
header-name	The user-specified header name in HTTP GET/POST messages.
reg-exp-string	A regular-expression or normal string for the header value.

Use the **no** form of the command to delete the mapping. The following example shows the syntax for such a deletion.

```
aim asset-manager
    no device-class <class-name>
        no match http { <user-agent> | <host> | <uribase> | <param> | header
<header-name>}  <reg-exp-string>
        no priority <num:0-255>
```

Configuration Example

```
(conf) aim asset-manager
(aim-conf) device-class iPhone4
(device-class-conf) match http user-agent “\w+iOS*4.0”
(device-class-conf) match http param “begin\=”
(device-class-conf) priority 5
```

```
    (conf) aim asset-manager
    (aim-conf) device-class iPad
    (device-class-conf) match http user-agent reg-exp "iPad"
    (device-class-conf) match http param reg-exp "begin\="
    (device-class-conf) priority 3
```

Popularity Configuration

Use popularity configuration to define popularity settings such as the threshold for triggering adaptation, the video selection, and so on.

Syntax

```
aim popularity class <class name>
    threshold 1min <value> 1hr <value> 4hr <value> 1day <value>
        expiry <number seconds>
            match-rule [host | uribase | param | http-header <header type>] <regexp>
```

The following table describes the parameters used in this command.

Syntax Description

`class name`	Popularity class name.
`thresholds`	Values for per minute, per hour, per 4-hour interval, and per day (range 1 to 2147483647).
`expiry`	Content expiration time in seconds (range 1 to 2147483647).
`match-rule`	<header type> can be any type defined in the HTTP header. Refer to HTTP parser section.
`regexp`	Pattern string

Use the **no** form of this command to delete a popularity class definition.

```
no aim popularity class <class name>
    no threshold 1min <value> 1hr <value> 4hr <value> 1day <value>
        no expiry <number seconds>
            no match-rule [host | uribase | param | http-header <header type>] <regexp>
```

Configuration Example

```
    (conf) aim asset-manager
        (aim-conf) aim popularity class popclass
        (aim-conf-popclass) threshold 1min 10 1hr 100 4hr 200 1day 500
                  (aim-conf-popclass) expiry 6000
                  (aim-conf-popclass) match-rule host "*youtube*"
```

Blacklist/Whitelist

Use the following CLI command to configure the blacklist or whitelist as needed.

Syntax

```
cae source-content-group {blacklist | default | whitelist}
```

The following table describes the parameters used in this command.

Syntax Description

`blacklist`	Configure blacklist
`deafult`	Restore the default setting
`whitelist`	Configure whitelist

AIM Show Commands

AIM Device Class Information

Use this command to display information for all AIM device classes or for a specific AIM device class.

Syntax

```
show aim device-class {all | name <device-class-name>}
```

Use the **all** option to show information for all device classes, or **name** to show information for a particular device class specified in <device-class-name>.

Example

```
switch# show aim device-class name device-class1
Device Class: device-class1
Priority    : 1
Total 2 matching rules
Match User Agent : Android
Match host : google.com
```

Note The show aim database command does not support the Beginning (Beg) option.

AIM Popularity Class Information

Use this command to display information for all AIM popularity classes or for a selected AIM popularity class.

Syntax

```
show aim popularity-class {all | name <popularity-class-name>}
```

Use the **all** option to show information for all popularity classes, or **name** to show information for a particular popularity class specified in <popularity-class-name>.

Example

```
switch# show aim popularity-class all
       Popularity class: pop-class-1
            Match-rule: Host (.*video.*)
            Expiry time: 1800 seconds
            Threshold:
                    1-minute: 10
                    1-hour: 50
                    4-hour: 200
                    1-day: 1000
switch#
```

AIM Database Information

Use these commands to display information for one or all entries in the AIM database, and to display the current state of the entry or entries.

Show AIM Database All

Use this command to display detailed information ofAIM records. Using this command alone displays only the first 2,000 records. Subsequent records can be viewed by reissuing the command and providing an offset.

Syntax

```
show aim database all [offset <#>]
```

Show AIM Database Entry

Use this command to display the specified information for the applicable entries in the AIM database.

Syntax

```
show aim data entry {asset-descriptor <value> | device-class <value> |
adaptation-profile-index <value> | all}
```

The following table describes the parameters used in these commands.

Syntax Description

`asset-descriptor`	Show the AIM database entry with the specified asset descriptor.
`device-class`	String the AIM databsae entries with the specified device class.
`adaptation-profile index`	Show the AIM database entries with the specified API value.

Example

```
List the following columns:

Create-time || state  || b/w gain || content-time || AD ||  popularity-class || DC ||
video-bit-rate ||
Quality-Index || Aggregated-hit-count || Hits per minute for 1 min || Timestamp for 1
min || Hits per 1 hr || Timestamp for 1 hr  || Hits per 4 hour || Timestamp per 4 Hr
|| video length in bytes  || Expiry Time stamp
switch# show aim database entry all
AD: ba6be7f700201302220932150 0f6ddd3
        Popularity class: default POP Class
        Entry State: READY, Content status: URL Available
        Entry created at: Wed Dec 31 16:33:31 1969
        Content Expiry: Wed Dec 31 16:33:31 1969
        Content length: 0, BW gain: 0 Bitrate: 0
        Aggr hit count: 16
        Hits: per min 4, per hour 16, per 4 hours 16, per day 16
        Timestamps:
                Per 1 minute: Mon Oct  3 15:17:07 2011
                Per 1 hour: Mon Oct  3 15:10:07 2011
                Per 4 hours: Mon Oct  3 15:10:07 2011
                Per 1 day: Mon Oct  3 15:10:07 2011

switch#
```

Show AIM Database Summary

This command provides the number of AIM records in the database along with a breakdown of the number of records in each state.

Syntax

```
show aim database summary
```

Show AIM Database State

Use this command to display the entries in the AIM database that are currently in a specified state.

Syntax

```
show aim database state {1 | 2 | 3 | 4}
```

The following table describes the parameters used in these commands.

Syntax Description

`1`	Show Created AIM database entries only.
`2`	Show Adapting AIM database entries only.
`3`	Show Ready AIM database entries only.
`4`	Show Ready-Adapting AIM database entries only.

AIM Statistics

Use this command to display statistics for the AIM database. You can display all statistics or a specified subset of statistics.

Syntax

```
show aim statistics {content-retrieval | content-adaptation | http | all |
content-popularity-update}
```

Note This command does not support the use of single quotes for the domain value.

Syntax Description

`content-retrieval`	Show AIM content-retrieval statistics.
`content-adaptation`	Show AIM content adatpation statistics.
`http`	Show AIM HTTP statistics.
`all`	Show all AIM statistics.
`content-popularity-update`	show all AIM content-popularity updates.

Example

```
sjst67#show aim statistics all

HTTP Statistics:
    Total parsed requests: 6
    Total parsed responses: 6
    Total parsed request errors: 0
    Total parsed response errors: 0
    Total bad messages received: 0
    Total unsupported HTTP fields received: 0

Content Retrieve Statistics:
    Total CRREQs received:           3
    Total CRREQs matching blacklist: 0
    Total CRREQs not matching whitelist 0
    Total CRRSPs sent:               3
    Bad CRREQ message format: 0
    Invalid CRREQ req code: 0
    CRREQ update receive queue empty: 497882
    CRREQ update receive fail: 0
    CRREQ update receive success: 3
    CRREQ update send fail: 0
    CRREQ update send success: 3
    Bad HTTP request headers: 0
    Bad HTTP response headers: 0
    No device class matched: 0
    Asset descriptor mismatch: 0
    Invalid API: 0
    No popularity class matched: 0
    Zone unknown: 3
    Total database read errors: 0
    Total TCP send errors: 0
    CRREQ decode errors: 0
    CRRSP encode errors: 0
    TCP data errors: 0

Content Adaptation Statistics:
    CAREQ sent: 1
    CAREQ send failed: 0
    CAIND received: 1
    CANOT received: 0
    CAIND failed to process: 0
    CANOT failed to process: 0
    CAE Manager message received: 1
    CAE Manager message failed: 0
    Access content expiry/invalid: 0
    Total created to adapting: 0
    Total to adapting to ready: 0
    Total ready-adapting to ready: 0
    CAREQ encode errors: 0
    CANOT/CAIND decode errors: 0
    Database lock errors: 0

Content Status Update Statistics:
    Total CSUPDs received: 0
    Online Xcode Failure received: 0
    NAS File Missing Failure received: 0
    BAD CSUPD message format: 0
    CRREQ decode errors: 0
    Invalid CSUPD status code: 0
    No device class matched: 0
    Asset descriptor mismatch: 0
    Invalid API: 0
    Total database write errors: 0
    Total database read errors: 0

Content Popularity Update Statistics:
    Total CPUPDs received: 3
    Total CPUPDs matching blacklist: 0
    Total CPUPDs not matching whitelist: 0
    Bad HTTP request headers: 0
    Bad HTTP response headers: 0
    No device class matched: 0
    Asset descriptor mismatch: 0
    Invalid API: 0
    No popularity class matched: 0
    Total database read errors: 0
    Total database write errors: 0
    CPUPD decode errors: 0

sjst67#
```

AIM Clear Commands

AIM Clear Statistics

Use this command to remove all AIM statistics from the database.

Syntax

```
clear aim statistics all
```

Syntax Description

all	Clears all AIM statistics.

Example

```
CD4-OFAM#clear aim statistics all
```

AIM Clear Database Rows

Purpose

Use this command to remove all rows from the AIM database, or only rows that match a specified condition.

Syntax

```
clear aim database {aim-id <value> | all | asset-descriptor <value> | state <value>}
```

Example

```
CD4-OFAM#clear aim database all
```

Syntax Description

aim-id	Clear AIM database rows that match the AIM ID.
all	Clear all AIM database rows.

`asset-descriptor`	Clear AIM database rows that match the asset descriptor.
`state`	Clear AIM database rows that match the state.

Purpose

Use this command to display all logs of a specified type from the AIM database for debugging purposes.

Syntax

```
debug aim all {detail | error | trace}
```

AIM Debug

Syntax Description

`detail`	Display AIM log level detail.
`error`	Display AIM log level error.
`trace`	Display AIM log level trace.

Web Engine CLI

Web Engine Configuration

The service engine (SE) with WebEngine enhancement for CAE is part of the CAE cluster. This command allows the WebEngine MVG helper to connect to the AIM.

```
cae aim primary-ip <x.x.x.x> [secondary-ip <x.x.x.x>] [port 8001]
```

Note From the perspective of CDSM, this is a per-node or per-device configuration.

Web Engine Show Statistics

Use these commands to display WebEngine statistics.

Syntax

```
show statistics web-engine <detail>
```

where <detail> is an optional parameter used to request a more detailed output.

Note This command does not support the use of single quotes for the domain value.

Note We advise against using the Cache Miss and Cache Hit counters to determine how frequently videos are accessing offline fetched content. Instead, we suggest using Transcoded Offline Content and Transcoded Online Content statistics to measure how often offline data is being accessed.

Examples

General Form

```
#show statistics web-engine

HTTP Request Info Statistics
-----------------------
Num Lookups                   :                        12066
Preposition Hit               :                            0
Alien Hit                     :                            0
Cache Hit                     :                            0
Cache Miss                    :                          862
Partial Cache Hit             :                            0
Cache Bypass                  :                        13837
Live Miss                     :                            0
Live Hit                      :                            0
ASX Meta Response             :                            0
Error Response Miss           :                            1
Error Response Hit            :                            0
// The following are new CAE outputs
Serving Xcoded Offline        :                           20
Serving Xcoded Online         :                           25
```

Detailed Form

```
show statistics web-engine detail

HTTP Request Info Statistics
-----------------------
Num Lookups                   :                          114
Preposition Hit               :                            0
External Hit                  :                            0
Cache Hit                     :                            0
Cache Miss                    :                          114
Partial Cache Hit             :                            0
Cache Bypass                  :                            0
Live Miss                     :                            0
Live Hit                      :                            0
ASX Meta Response             :                            0

HTTP Request Type Statistics
-----------------------
Get Requests                  :                          114
Post Requests                 :                            4
Head Requests                 :                            0
Put Requests                  :                            0
Delete Requests               :                            0
Trace Requests                :                            0
Options Requests              :                            0
Connect Requests              :                            0
Patch Requests                :                            0
Unknown HTTP Method Requests  :                            0
Range Requests Received       :                           15
Range Requests Sent           :                           20
Revalidation Requests Received :                          15
Revalidation Requests Sent    :                           20
Liveness Query                :                            0
CAE Liveliness Requests       :                            0
WMT(http) Redirected Requests  :                           0
Local Requests                :                            0
Play Live Requests            :                            0
Total Outgoing Requests       :                          123

HTTP Authorization Statistics
----------------------
```

```
Authorization Allow           :                          0
Authorization No Cache        :                          0
Authorization Force Revalidate :                         0
Authorization Deny            :                          0
```

Web Engine Show Cached Content

Use this command to display local Web Engine cached content.

Syntax

```
show cache content
```

Web Engine Debug

Purpose

Use this command to display all logs of a specified type from the Web Engine database for debugging purposes. Error logs are displayed by default, but detail or trace logs also may be specified.

Syntax

```
debug web-engine {detail | error | trace}
```

Syntax Description

detail	Display Web Engine log level detail.
error	Display Web Engine log level error (default).
trace	Display Web Engine log level trace.

CAE Offline Manager CLI

General Settings

The following settings can be made for Offline Manager:

- Own Server Port – IPC TCP listening port for the AIM
- Original Input Directory – location where Fetcher saves its downloaded original files
- Transcoding Output Directory – location where CTM Server saves transcoded files
- Transcoder Job Request Timeout – time Offline Manager waits for each transcoding job request

Default settings for each parameter are in place, but can be modified using CLI commands as follows to suit the needs of each deployment.

```
#cae offline-mgr server port 8002 // default to 8002
#cae input-location directory input
#cae output-location directory output
#cae xcode timer 2200 // default to 1800
```

From the perspective of the AIM process, Offline Manager is a TCP server. This is a per-device configuration and applies to the location where Offline Manager is running.

OFAM Enable-Disable

You can enable and disable OFAM processes using CLI commands, as shown in the following examples.

Example

```
CAE(config)#cae ofam mode-enable //This can only be entered if cae enable is configured.
once configured, it will launch the OFAM (AIM, Offline Manager, and Fetcher) processes.

CAE(config)#no cae ofam-mode enable //This command stops the OFAM (AIM, Offline Manager,
and Fetcher) processes.

CAE(config)#cae enable //This command enables the CAE feature. Whether OFAM processes are
launched depends on if "cae ofam-mode enable" is configured.

CAE(config)#no cae enable //This command disables CAE processes, including the OFAM
processes.
```

Fetcher IP and Port

By default, the Offline Manager always connects to a local Fetcher - that is, one running on the same node. Offline Manager and Fetcher connect using the default port. This is a per-device configuration, and applies to the location where Offline Manager is running.

Note The default port is 8003.

You can choose to use an external Fetcher by entering its corresponding IP address and port. For the purpose of defining the TCP connection between Offline Manager and Fetcher, Offline Manager is a TCP client and Fetcher is a TCP server.

Example

If Offline Manager and Fetcher are located in different nodes, or if a non-default port is used, the following CLI serves the purpose:

```
CAE(config)#cae offline-mgr fetcher <ip a.b.c.d> [port 8002]
#cae offline-mgr fetcher ip 172.25.128.43 port 8003
```

This line can be repeated as needed in order to configure multiple Fetchers.

Original Input

This is the location where Fetcher saves the content from the original server.

```
CAE(config)#cae input-location directory input
```

From the perspective of CDSM, this is a per-node configuration so that different nodes can save files to different directories. This command is synchronized to the CDSM GUI.

Transcoded Output

This is the location where the CTM node saves its transcoded output video content.

```
CAE(config)#cae output-location directory output
```

From the perspective of CDSM, this is a per-node configuration so that different nodes can save files to different directories. This command is synchronized to the CDSM GUI.

Transcoder Timer

Use this command to specify the time that Offline Manager waits for each job to be submitted to the CTM server.

```
CAE xcode timer 2200 // wait 2200 seconds
```

This command is synchronized to the CDSM GUI.

Adaptation XML File

The adaptation XML file defines the transcoding rules used by both the Offline Manager and the Web Engine. The CDSM uses this CLI command to inform both applications of a new adaptation XML file rule.

```
CAE adaptation-rule file /state/contentAdaptFile/cae_v2.xml
```

Note A file configured locally with this command is not reflected in the CDSM GUI because the CLI cannot upload the content of the adaptation file into CDSM.

Offline Manager Show

Offline Manager Statistics show

Examples

```
#show cae offline statistics //or #show cae offline-mgr statistics

Offline-Mgr Progressive Statistics
    CAREQ Requests Recv                  :                 6
    CAIND Response Sent                  :                 0
    CANOT Response Sent                  :                 6
    Fetch Requests Sent                  :                 0
    Fetch Response Recv                  :                 0
    Transcode Job Requests               :                 0
    Transcode Job Response               :                 0
    CAREQ Requests Recv failed           :                 0
    CAIND Response Sent failed           :                 0
    CANOT Response Sent failed           :                 0
    Fetch Requests Sent failed           :                 0
    Fetch Response Recv failed           :                 0
    Transcode Job Requests failed        :                 0
    Transcode Job Response failed        :                 0

Offline-Mgr HLS ABR Statistics
    Manifest CAREQ Requests Recv         :                 0
```

```
        Manifest CAIND Response Sent         :                 0
        Manifest CANOT Response Sent         :                 0
        Manifest Fetch Requests Sent         :                 0
        Manifest Fetch Response Recv         :                 0
        Chunk Fetch Requests Sent            :                 0
        Chunk Fetch Response Recv            :                 0
        Chunk Transcode Job Requests         :                 0
        Chunk Transcode Job Response         :                 0
        Manifest CAREQ Requests Recv failed  :                 0
        Manifest CAIND Response Sent failed  :                 0
        Manifest CANOT Response Sent failed  :                 0
        Manifest Fetch Requests Sent failed  :                 0
        Manifest Fetch Response Recv failed  :                 0
        Chunk Fetch Requests Sent failed     :                 0
        Chunk Fetch Response Recv failed     :                 0
        Chunk Transcode Job Requests failed  :                 0
        Chunk Transcode Job Response failed  :                 0
```

Note This command does not support the use of single quotes for the domain value.

Offline Manager Job show

This command displays one or more CAE offline jobs currently in progress.

Syntax

```
#show cae offline session all
```

Where <asset-descriptor> is an optional parameter that lets you to display details for a single job.

Example 1

```
#show cae offline session all
Fetching   ASSEST-ID-1 www.youtube.com/video.mp4
Xcoding    ASSEST-ID-2 www.youtube.com/video.mp4
```

Example 2

```
#show cae offline session asset-descriptor <value>
Asset-Desc:   abbbemeppdnnssaaa2345
URL:          www.youtube.com/video.mp4
State:            Xcoding
Device Class:     iPhone4
API:              4
Xcode Template: CAE-iphone-medium-H.264-400x224-150kbps
```

Offline Manager Clear

```
#clear cae offline statistics  [domain www.youtube.com]
```

Offline Manager Debug

```
#debug cae offline error
#debug cae offline detail
#debug cae offline trace
#
```

Fetcher CLI

Configuration

With respect to Offline Manager, fetcher is a TCP server and its port is configurable.

```
CAE(config)#cae fetcher port 8008 // default 8003
```

The Fetcher can also define its timeout value for each HTTP request, as follows:

```
#cae fetcher timer 1800 // in seconds
```

Note This is a per-device configuration, and applies to the location where the Fetcher process is running. This configuration is implemented with CDSM GUI.

Show

```
#show cae fetcher statistics

Fetcher Statistics
------------------
Fetch Requests Recv                     :                 0
Fetch Requests Recv failed              :                 0
Fetch Response Sent                     :                 0
Fetch Response Sent failed              :                 0
HTTP Req Sent                           :                 0
HTTP Req Sent failed                    :                 0
HTTP Rsp Received                       :                 0
HTTP Rsp Received failed                :                 0
ABR Statistics
------------------
Manifest Fetch Requests Recv            :                 0
Manifest Fetch Requests Recv failed     :                 0
Manifest Fetch Response Sent            :                 0
Manifest Fetch Response Sent failed     :                 0
Manifest HTTP Req Sent                  :                 0
Manifest HTTP Req Sent failed           :                 0
Manifest HTTP Rsp Received              :                 0
Manifest HTTP Rsp Received failed       :                 0
Chunk Fetch Requests Recv               :                 0
Chunk Fetch Requests Recv failed        :                 0
Chunk Fetch Response Sent               :                 0
Chunk Fetch Response Sent failed        :                 0
Chunk HTTP Req Sent                     :                 0
Chunk HTTP Req Sent failed              :                 0
Chunk HTTP Rsp Received                 :                 0
Chunk HTTP Rsp Received failed          :                 0
```

Note This command does not support the use of single quotes for the domain value.

Debug

```
#debug cae fetcher error
#debug cae fetcher detail
#debug cae fetcher trace
```

GLOSSARY

A

ABR Adaptive Bit Rate.

AD Asset descriptor; an identifier for original video.

AIM Asset Information Manager; a CAE process that maintains a database of video assets.

API Application Programming Interface; Adaptation Profile Index.

Armada Former product name for Cisco Transcode Manager (CTM).

C

CAE Content Adaptation Engine; the original name for VDS-OE, which still appears in some GUI elements.

CAE Controller CAE component responsible for handling the interface to MVG, managing transcoding operations through the CAE and CTM, and video delivery.

CAIND Content Adaptation Indication; a message sent from the Offline Manager to the AIM when content has been adapted by the transcoder.

CAL Content Abstraction Layer.

CAREQ Content Adaptation Request; a message sent from the AIM to the Offline Manager to initiate transcoding.

CDN Content Delivery Network.

CDS Content Delivery System.

CDSM Content Delivery System Manager.

CLI Command Line Interface.

CRREQ Content Retrieval Request; an IPC message sent from the CAE-SE (Web Engine) to the AIM to query whether offline transcoded content is available.

CRRSP Content Retrieval Response; an IPC message sent from the AIM to the CAE-SE to indicate whether offline transcoded codent is available, and if so, the location of the content.

CTM Cisco Transcode Manager; formerly called Armada.

Cisco Unified Fabric Techology that combines LAN and SAN networks into a single physical infrastructure using Fiber Channel over Ethernet (FCoE). By virtue of its use of 10 gigabit Ethernet (10-GE) converged network adapters (CNAs), this technology streamlines cabling, interface, and adapter requirements and provides increased capacity and enhanced redundancy at much lower total cost of ownership.

H

HA High Availability.

HLS HTTP Live Streaming; an Apple technology for streaming internet video.

Hypervisor Also called a virtual machine monitor (VMM); a virtualization application that allows multiple operating systems to run concurrently on a host computer. Type 1, or native, hypervisors are software systems that run directly on the host hoardware as a hardware control and gues operating system monoitor. Examples include VMWare ESX/ESXi Server, Xen, and Microsoft Hyper-V. Type II hypervisors run within a conventional operating system environment, such as Linux, and do not offer the scalability required for next-generation IP video applications.

I

IPC Inter-Process Communication.

K

KPI Key Performance Indicator.

M

MDC Media data center; a data center that also including decoders, encoders, and other equipment needed to support IP video ingest, storage, conditioning, and distribution. The Cisco MDC architecture is designed to host multiple services spanning a wide range of video and subscriber applications while providing the necessary access, redundancy, isolation, and security measures.

MVG Mobile Video Gateway.

N

NTP Network Time Protocol.

O

OFAM Offline Asset Manager; CAE component that combines the AIM, Offline Manager, and Fetcher processes.

Offline In the context of CAE, refers to video content that has been transcoded and stored before it is delivered to a user device.

Online In the context of CAE, refers to video content that is transcoded in real time as it is being delivered to a user device.

OS Operating System; Origin Server.

Q

QoS Quality of Service.

R

RAN Radio Access Network.

RAT Radio Access Technology.

S

SE Service Engine.

SIP Session Initiation Protocol.

SR Service Router.

SS Smooth Streaming; a Microsoft technology for streaming internet video.

T

TCPO TCP Transport Optimization.

TPO Transport Optimization such as TCPO or HTTP Data Optimization.

Transcode To convert the encoding scheme for a video to a different scheme for compatability with a specific system or device.

Transrate To convert the data rate of an encoded video stream for compatibility with a specific system or device.

U

UCS Unified Computing System.

UE User Equipment; especially, a mobile terminal.

V

VDS-OE Video Distribution Suite - Optimization Engine.

Virtualization The instantiation of one or more operating system environments in self-contained virtual machines that are independent of the computer hardware on which they run. This allows the operating system and its applications to be copied or moved from one hardware platform to another, and for multiple virtual machines to run on the same physical data-center server in isolation from each other, to improve the utilization of network resources.

VOD Video on Demand; video content offered for sale by a service provider or partner such as AT&T U-Verse or Verizon FiOS.

X

X-header In SIP, a header used to send non-standard information.