Cisco MediaSense User Guide, Release 10.0(1)

First Published: December 12, 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

CONTENTS

Preface

Preface ix

Audience ix

Documentation conventions ix

Related documentation x

Documentation and service requests x

Documentation feedback xi

CHAPTER 1

MediaSense Features and Services 1

Network services 1

Feature services 2

Search and Play 3

Search for, play, or download a recorded call 3

Architecture 5

Unified Communications Manager deployments 5

Cisco Unified Border Element deployments 6

Unified CM and CUBE scenario differences 7

Supported deployments 9

MediaSense cluster deployments 9

Single-server deployments 10

Dual-server deployments 11

Three-server deployments 12

Four-server and five-server deployments 13

MediaSense high availability deployments 14

Data replication considerations 14

Data replication and recovery for primary or secondary node 15

Deployment considerations for high availability 15

Failure condition considerations 16

MediaSense requirements 17
Media storage requirements 17
Hardware requirements 17
Software requirements 18
License requirements 18
Other requirements 18
Port usage 18

CHAPTER 2 Install or Upgrade MediaSense 21
Install MediaSense 21
Pre-installation tasks and tools 21
Installation and configuration worksheet 21
Answer files for unattended fresh installations 23
Navigate the installation wizard 23
Installation process 24
Install MediaSense and Unified OS 24
Post-installation tasks 27
Complete setup for primary server 28
MediaSense server configuration 30
Details for secondary and expansion servers 31
Finish setup for subsequent servers 31
System verification 32
Unified CM provisioning for MediaSense 33
Set up call control service connection 33
Disable iLBC and iSAC for recording device 35
Upgrade MediaSense 35
Upgrade considerations 35
Upgrade cluster to release 10.0(1) 37
Node upgrade procedures 38
Upgrade nodes from a local source 38
Remote sources 39
Upgrade nodes using Unified OS Administration 39
Upgrade nodes using Unified OS CLI 40
Rollback cluster 41
Install COP files 42

Language pack 43

CHAPTER 3 Administer and Configure MediaSense 45

Access MediaSense Administration 45

Single sign-in 46

MediaSense Administration 46

Unified CM configuration 47

Unified CM user information and MediaSense setup 47

Select AXL service providers 47

Select call control service providers 48

Replace Unified CM service providers 49

MediaSense setup with Finesse 50

Cisco Finesse configuration 50

Provision users for MediaSense deployment 50

MediaSense API users 50

API user configuration 51

Storage management agent 51

Pruning Options 52

Prune Policy Configuration 53

Storage threshold values and pruning avoidance 54

System thresholds 56

View disk space use 56

Storage use information obtained using HTTP 57

Storage use information obtained by using Unified RTMT 57

Incoming Call Configuration 58

Add Incoming Call Rule 58

Edit Incoming Call Rule 59

Edit System Default Incoming Call Rule 59

Delete Incoming Call Rule 60

Media File Management 60

Media File Details 61

Add Media File 62

Edit Media File 63

Redeploy Media File 63

Delete Media File 63

Refresh media file 64
MediaSense server configuration 64
Media partition management 65
Configure Media Partitions 65
Event management 66
Enable event forwarding 66
MediaSense setup with Cisco Unified Border Element 67
Manage Unified CM users 67
Cisco MediaSense provisioning for CUBE 67
CUBE and MediaSense setup 68
CUBE gateway accessibility 68
CUBE view configuration commands 68
Global-level interoperability and MediaSense setup 69
Setup global level 69
Dial-peer level setup 71
Set up CUBE dial-peers for MediaSense deployments 71
CUBE deployments log commands 74
Access MediaSense Serviceability 75
MediaSense Serviceability 75
Trace setup 76
Trace files 76
Trace log levels 76
Trace flags 77
Trace file location 78
Set up trace file information 79
Trace file interpretation 79
Performance logging 79
Dump trace parameters 80
Serviceability tools 80
Control center network services 81
Manage network services 81
Control center feature services 81
Manage feature services 82
Media service call control service or database service reactivation 82
Access serviceability user interface for other servers in cluster 82

Unified RTMT administration 83
Unified RTMT installation and setup 83
Download the Unified RTMT plug-in 83
Unified RTMT upgrade 84
Unified RTMT multiple copy installations 84
Server status monitoring 84
Performance monitoring counters 85
Unified RTMT for performance monitoring 85
System condition and perfmon counter alerts 85
AMC service and Unified CM setup 87
Trace and log central Unified RTMT setup 88
File collection 89
Crash dump collection 89
Remote browse folder names and services 89
Perfmon agent and counters 90
Server IP address changes 94
Prepare system for IP address change 94
Change IP address of primary server 95
Change IP address of secondary server 98
Change IP address of expansion server 100
Change multiple IP addresses in a MediaSense cluster 102
MediaSense command line interface (CLI) commands 104
CLI access 104
Utils commands 105
utils media recording_sessions 105
utils service 105
utils system maintenance 106
Run commands 107
run db_reset_replication 107
run db_synchronization 107
Set network commands 108
set network cluster server ip 108
set network cluster primary ip 109
set network cluster secondary ip 109
set network ip eth0 110

Show commands 110
show db_synchronization status 111
show network cluster 111
show tech call_control_service 112

CHAPTER 4 Troubleshoot MediaSense 113

CHAPTER 5 MediaSense Terminology 115
Play back 115
Blog recording 116
Media forking 116
Sessions and recording sessions 116
Glossary 117

Preface

This document describes the Cisco MediaSense network-based media services platform that supports the recording, playback, live streaming, and storage of media.

- Audience, page ix
- Documentation conventions, page ix
- Related documentation, page x
- Documentation and service requests, page x
- Documentation feedback, page xi

Audience

This document is written for system administrators who have the domain-specific knowledge required to install, set up, configure, maintain, and troubleshoot MediaSense.

System administrators need experience with or training in Java to make the best use of the capabilities of MediaSense and of the entire Cisco Unified Communications family of products.

Documentation conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit > Find** . • Click **Finish**.

Convention	Description
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco CRS Installation Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems,Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Related documentation

Documentation for MediaSense is available on Cisco.com. For more information about other documents in the MediaSense documentation set see the *Cisco MediaSense Documentation Guide* at http://www.cisco.com/en/US/products/ps11389/products_documentation_roadmaps_list.html .

Documentation and service requests

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

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

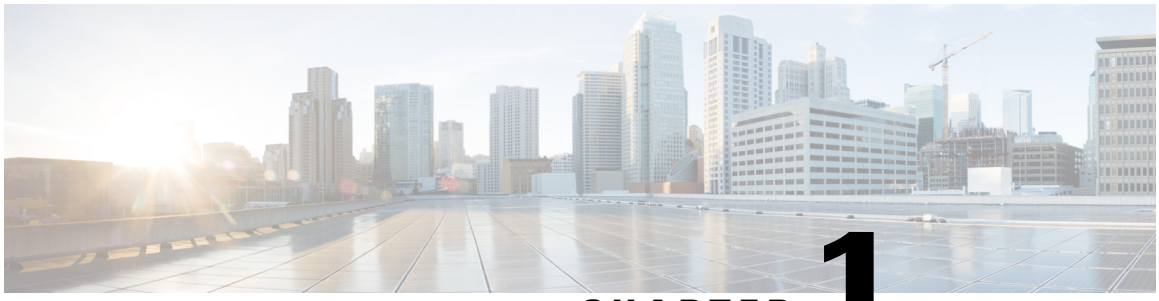
Subscribe to *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Documentation feedback

You can provide comments about this document by sending an email to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.



CHAPTER 1

MediaSense Features and Services

MediaSense is the media-capture platform for Cisco Unified Communications. It can be used to record calls in Cisco and non-Cisco contact centers; however, non-Cisco contact centers must use the Cisco Unified Border Element (CUBE) as the ingress point.

MediaSense can be used by compliance recording companies whose regulatory environment requires all sessions to be recorded and maintained. These recordings can later be used by a compliance auditor or a contact center supervisor to resolve customer issues or for training purposes. The recordings can also be used by speech analytics servers or transcription engines.

MediaSense uses Unified Communications Manager (Unified CM) to provide user-authentication services. It uses Web 2.0 application programming interfaces (APIs) to expose its functionality to third-party customers to enable them to create custom applications. The product is supported on Microsoft Windows 7 and the Apple Mac OS.

- Network services, page 1
- Feature services, page 2
- Search and Play, page 3
- Architecture, page 5
- Unified Communications Manager deployments, page 5
- Cisco Unified Border Element deployments, page 6
- Supported deployments, page 9
- MediaSense cluster deployments, page 9
- MediaSense high availability deployments, page 14
- MediaSense requirements, page 17
- Port usage, page 18

Network services

Network services include the following:

- **Cisco MediaSense Administration**: Enables you to configure MediaSense using a graphical user interface.
- **Cisco MediaSense Serviceability Administration**: Enables you to configure the MediaSense Serviceability application using a graphical user interface.
- **System Service**: Enables you to control service operations within the MediaSense clusters. This service manages the clustering and setup functionality for the secondary server and expansion servers.
- **Perfmon Agent**: Enables you to control the performance monitoring infrastructure within the MediaSense Serviceability Administration interface. The Java Management Extensions (JMX) technology, which allows you to manage and monitor applications and other system objects, is represented by objects called Managed Beans (MBeans). The Perfmon Agent retrieves the counter values from the JMX MBeans and writes them to the Unified CM database.
- **Diagnostics Service**: Enables you to troubleshoot and debug MediaSense. This service is available in all MediaSense servers.

In the MediaSense and Unified OS user interfaces, each MediaSense service name is preceded by the product name. To avoid redundancy in this document, service names are sometimes referred to without the preceding product name.

Network services are started automatically after installation in each server in the cluster. If advised to do so by Cisco support personnel, network services can be stopped.

Feature services

MediaSense contains the following feature services:

- **Configuration service**: saves and updates all changes made to the MediaSense configuration database. Each multiple-server cluster can have only two instances of the configuration service, one instance is in the primary server and the other instance is in the secondary server. If a cluster has more than two servers, the expansion servers cannot have a configuration service.
- **API service**: processes API requests and enables communication between the user interface and the server. You can enable the API service only after the database service is enabled. Each multiple-server cluster can have only two instances of the API service, one instance is in the primary server and the other instance is in the secondary server. If a cluster has more than two servers, the expansion servers do not have an API service.
- **Database service**: contains and controls the meta database and the configuration database. Each multiple-server cluster can only have two instances of the database service, one instance is in the primary server and the other instance is in the secondary server. Each server writes data only to its local database. The primary and secondary servers interact to synchronize data.
- **Storage management agent (SM agent)**: monitors the overall storage in each server in the cluster and generates threshold events based on disk usage. This service is available in all servers and should be activated before the media service and call control service.
- **Media service**: receives, saves, and plays back media. The media service must be enabled before the call control service. This service is available in all servers in the cluster.
- **Call control service**: coordinates call receiving and recording. The call control service can only be enabled if the media service is already enabled. This service is available in all servers in the cluster. The

call control service is referred to as a SIP trunk in the Unified CM user interface and Unified CM documentation.

All feature services are installed on the primary and secondary nodes (servers) in a cluster. Expansion nodes have only the media service, call control service, and SM agent.

Search and Play

After MediaSense is installed and configured, use the Search and Play application to search for specific media files, play them, or download them to your desktop.

Access the Search and Play application from

- a Firefox or IE9 browser at URL https://<hostname>:8440/mediasense

  or

- Click the **Cisco MediaSense Search and Play** link from the main MediaSense access screen at URL http://<MediaSense hostname>.

Note Before launching Search and Play, you'll need to install the 32-bit version of JDK on Windows OSs and the 64-bit version on Macs. Also, ensure that you have JDK7 update 25 or later installed.

The MediaSense media player is implemented as a downloadable Java application. Due to recent security enhancements in Java, users are asked to accept a pop-up security warning every time the Java application is executed; meaning that users must accept a security warning every time a recording is played.

Since the application does not run as part of the browser executable, it is subject to the security requirements of the Java Virtual Machine (JVM) that is installed on the user's computer (rather than those of the browser). A troubleshooting tip provides instructions for setting up each client desktop where Search and Play is executed to avoid the warning (http://docwiki.cisco.com/wiki/Administration:_Search_and_Play_application_users_encounter_security_warning_before_each_playback#Search_and_Play_application_users_encounter_security_warning_before_each_playback).

Note The media player takes longer to start in IE9 than in Firefox. IE9 users may also see an option to open a downloaded jnlp file.

When prompted for login credentials, use the API user credentials defined on the MediaSense API User Configuration page of the Administration application.

Search for, play, or download a recorded call

There are multiple ways to search for recorded media files in the Search and Play window.

Procedure

Step 1 When you first access the Search and Play application, the page opens to the **Recent Calls** default search results (all calls within last 7 days). You may select the **Recent Calls** or **Active Calls** searches by clicking those tabs at any time.

Step 2 For a simple search, enter any combination of participant identifiers and tags in the search box and click **Search**.
Use a space to separate each entry; the delimiter is treated as an OR operator. The simple search defaults to searching for calls within the last 7 days.

Step 3 For an advanced search, enter values in any of the search properties from the **Search Recordings** drop down menu.
The search properties include:

- **SessionId—**The identifier of a recording session with one or more tracks associated with it. Enter a session identifier in the text box. Only one SessionId can be searched at a time.
- **Participants—**The identifier for recording session participants. Participants are identified by phone extension. Enter a participant identifier in the text box. Multiple participants can be searched by separating the identifiers with a comma. When multiple participants are defined, the search returns only those calls containing all of the participants (the delimiter is treated as an AND operator).
- **Tags—**Enter any text. Searches for tags are treated as CONTAINS, so entering a single letter results in all tags that contain that letter. Spaces used in the search box are considered part of the value being searched, not as a delimiter. Therefore, searching for two words separated by a space returns only those calls with a tag containing both words separated by a space.
- **XRef CI—**The recording session identifier. Enter a recording session identifier in the text box. Only one XRefCI can be searched at a time.
- **CCID—**The identifier of an individual track within a recording session. Enter a track identifier in the text box. Only one CCID can be searched at a time.
- **Range—**The date the recording session started. Select to search Within a specific time frame or Between a range of dates. If no time frame is selected, the system defaults to within the last 7 days

  When selecting a range of times, choose short time periods. Searches that result in large numbers of recordings may take an exceptionally long time to process and will impact system performance.
- **Duration—**Select a time unit, then use the slide bar to select the interval amount for the recorded session in seconds, minutes, or hours.
- **Show—**Use the check boxes to indicate if you want to search for completed calls, active calls, or calls with recording errors.

Step 4 Click **Search**.

- Click on the **Sort by** drop down menu to sort the files by age or duration.
- Click on the download icon to download a recording.
- Click on the play icon to play a recording.
- Users can select the number of results to display on each page and step through the result pages using the Previous and Next buttons.

Note When exiting the media player, users may receive an warning stating that the 'MediaSense player quit unexpectedly while using the lib... plug-in'. This warning may be reported as an error, but it is not an error and can be disregarded.

Architecture

MediaSense is part of the solution for Unified Communications and runs on Cisco Unified Operating System (Unified OS), Release 9.0.

MediaSense architecture contains the following components:

- Application layer:
  - The Search and Play application allows you to play back recordings.
  - APIs support real-time recording controls (such as hold, pause, and resume) for third-party applications.
  - Application and media APIs incorporate requirements from various industry partners and are published for use by third-party applications.
  - The API Service provides web service interfaces to enable applications to search for and retrieve recordings and associated session history and metadata. This metadata information is stored in the *Meta* database.
- Media processing layer:
  - The media service terminates media streams to be stored on a local disk for archiving and playback.
  - Running media service on all the servers in a deployment allows for load balancing.
- Network layer:
  - Gateway and session border controller (SBC) media forking and media forking at endpoints.
  - Integration with Cisco Unified Communications Manager (Unified CM) for audio recording.
  - Integration with Cisco Unified Border Element (CUBE) for audio and video recording.

Unified Communications Manager deployments

Unified Communications Manager (Unified CM) must be configured appropriately to direct recordings to MediaSense recording servers. This includes configuring a recording profile, various SIP parameters, and, because MediaSense uses the Administrative XML layer (AXL) to authenticate users, the Unified CM AXL service must be enabled on at least one of its servers.

A basic Unified CM deployment for MediaSense requires one of the phones to be configured for recording. If both phones are configured for recording, two separate recording sessions are captured. Media forked by a phone is sent to the recording device where the forked streams are captured. See the *Cisco MediaSense Solution Reference Network Design* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html for further details.

All Cisco IP Phones that MediaSense supports have a built-in bridge (BIB) that allows incoming and outgoing media streams to be forked. MediaSense makes use of this capability to record inbound and outbound forked media. For more details about media forking, see the Unified CM documentation at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Cisco Unified Border Element deployments

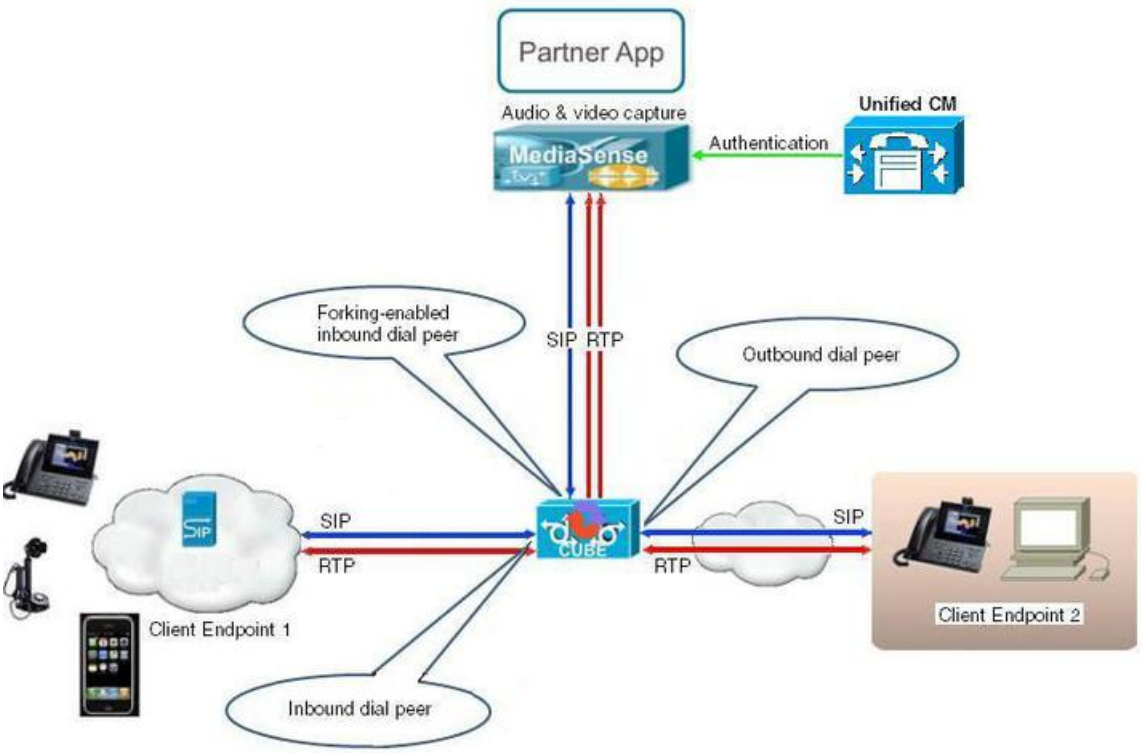
Cisco Unified Border Element (CUBE) is the Cisco session border controller (SBC) gateway that facilitates connectivity between independent VoIP networks by enabling SIP, H.323, VoIP, and video conference calls from one IP network to another.

MediaSense integrates with CUBE to enable recording without regard to the endpoint type. Because of this capability, MediaSense can use CUBE to record inbound and outbound media.

See the CUBE documentation for more information about CUBE.

- Generic CUBE configuration details are found at http://www.cisco.com/en/US/docs/ios/ios_xe/voice_cube_-_ent/configuration/guide/cube_ent/vb_book_xe.html.
- Specific recording configuration details are found at http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_proto/configuration/15-2mt/cube-network-based.html.

The following figure illustrates a MediaSense deployment with CUBE. Even in a CUBE deployment, MediaSense depends on Unified CM to provide authentication services.



In the preceding illustration, the real time protocol (RTP) carries voice data between the endpoints and CUBE. The session initiation protocol (SIP) carries call signaling information between the endpoints and CUBE. Two RTP unidirectional streams represent two audio streams forked from CUBE to MediaSense. Streams from CUBE to MediaSense are unidirectional because only CUBE sends data to MediaSense; MediaSense does not send any media to CUBE. CUBE has three dial-peers: inbound, outbound, and forking. (See Dial-peer level setup, on page 71 for more information.)

Typically, CUBE can fork only SIP-to-SIP calls. However, because you can use the same Cisco router as both a TDM-to-IP gateway and a media-forking device for call recording, you can also record incoming TDM or analog calls—if you have the required licensing and an appropriate IOS version. (For more information, see the CUBE documentation at http://www.cisco.com/go/cube.)

To use this feature, you must enable both gateway and border-element functionality in the device. You can configure the gateway to receive the TDM or analog call and then to feed the call back to itself as a SIP call with a different dialed number. When you configure this loop, the router actually handles each call twice. (This cuts the router capacity in half and CUBE can process only half as many calls.) For more information, see the *Media forking on a TDM gateway* section in the *Cisco MediaSense Developer Guide* at http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html and the MediaSense FAQ article at http://docwiki.cisco.com/wiki/FAQs_for_Cisco_MediaSense#How_to_Configure_a_TDM_Gateway_for_Media_Forking.

Unified CM and CUBE scenario differences

Unified CM is used to set up the recording profile and call control service connection (SIP trunk) with MediaSense. Similarly, with CUBE, the dial-peers and media class settings determine communication with MediaSense.

Note See the *Cisco MediaSense Solution Reference Network Design* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html for further details about CUBE media forking and UC endpoints media forking.

Almost everything that is not related to call signaling is the same between Unified CM scenarios and CUBE scenarios using MediaSense.

Regardless of whether MediaSense is deployed with Unified CM or CUBE; events, response codes, and parameter definitions are the same for both scenarios. All events, response codes, and parameters are explained in detail in the *Cisco MediaSense Developer Guide* at http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html.

Table 1: Unified CM and CUBE scenario differences

MediaSense feature	with Unified CM	with CUBE
Initiating recordings	The *direct outbound* recording scenario, which is initiated when a client calls the startRecording API, is supported with Unified CM deployments.	The *direct outbound* recording scenario, which is initiated when a client calls the startRecording API, is not supported with CUBE deployments.

MediaSense feature	with Unified CM	with CUBE
Recording	Two media streams are sent to MediaSense (called Track 0 and Track 1). Recording requires two phones with at least one phone configured for media-forking capabilities (two SIP invitations).	Recording uses SIP devices (referred to as SIP User Agent in CUBE). As long as the call is processed by CUBE as a SIP call, the endpoint can be of any type. Two media streams are sent to MediaSense. These two streams ultimately result in two tracks without any differentiation for Track 0 and Track 1.
Identifying tracks for *calling* versus *called* party See the FAQs for MediaSense website (How do you determine which track has the calling and which has the called party?).	The numerically smaller xRefCi parameter usually refers to the track of the calling party.	Track 0 contains the media stream corresponding to the dial-peer in which the media recording profile is configured.
Recording session See the *Cisco MediaSense Developer Guide* at http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html for details about recording sessions and hold/resume, pause/resume, transfer/conference commands.	If a call is placed on hold, the logical recording session is terminated. When a participant resumes the call, a new recording session is created.	The SIP Session may be updated multiple times with corresponding media track events. There is only one recording session even if the call is placed on hold and resumed multiple times.
Differences in the captured recording data See the *Cisco MediaSense Solution Reference Network Design* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html.	To obtain information such as the original calling number, called number, and type of call; see the Call Detail Records section in the *Unified Communications Manager Call Detail Records Administration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.	CUBE can store calls in an external database known as AAA - RADIUS. Calls can be searched by Cisco-GUID, which corresponds to the CCID in the MediaSense session data.
Mid-call codec change	Does not generate mid-call codec changes.	A new session starts.
Endpoint MAC address	Captured.	Not captured.
Recording media source	The endpoints provides the forked media.	CUBE provides the forked media.

Supported deployments

MediaSense supports the following deployments:

- One-server deployment: one active server.
- Two-server deployment: two active servers providing high availability.
- Three-server deployment: two active servers providing high availability and one expansion server to provide additional recording capacity.
- Four-server deployment: two active servers providing high availability and two expansion servers to provide additional recording capacity.
- Five-server deployment: two active servers providing high availability and three expansion servers to provide additional recording capacity.

Note UCS-E installations and all installations with less than 7 vCPUs are limited to one-server and two-server deployments.

In all the deployments, the installation and configuration of the primary server differs from the installation and configuration of the other servers in the same deployment. If you are configuring any server in a MediaSense deployment, be aware that the platform administrator configures the MediaSense application administrator username and password (in addition to the platform and security password). See Install MediaSense and Unified OS for further details.

Note The application administrator username and password must be the same on all servers in a MediaSense deployment. You can reset the application administrator username and password using the following CLI commands:

- `utils reset_application_ui_administrator_name`
- `utils reset_application_ui_administrator_password`.

MediaSense cluster deployments

In a MediaSense deployment, a cluster contains a set of servers with each server containing a set of services. Cluster architecture provides high availability (for recording but not for playback) and failover (if the primary server fails, there is automatic failover to the secondary server).

MediaSense functions only within local area networks (LAN). Wide are networks (WAN) are not supported. All MediaSense servers and Unified CM servers must be located in the same LAN. Within a LAN, the maximum round-trip delay between any two servers must be less than 2 ms.

The primary and secondary servers in a MediaSense deployment are synchronized when administrative changes are made on either server. Database replication copies the data automatically from the primary server to the secondary server, and vice versa.

The following cluster deployment rules are enforced by the installation and configuration procedures:

- All servers in the same cluster must run the same version of MediaSense.
- A MediaSense deployment can consist of one to five MediaSense servers. Each server in a cluster must always have a call control service, media service, and an SM agent.
- MediaSense supports any of the following combinations of servers:
  - One primary server.
  - One primary server and one expansion server.
  - One primary, one secondary server, and from one to three expansion servers.
- UCS-E installations and all installations with less than 7 vCPUs are limited to one-server and two-server deployments.

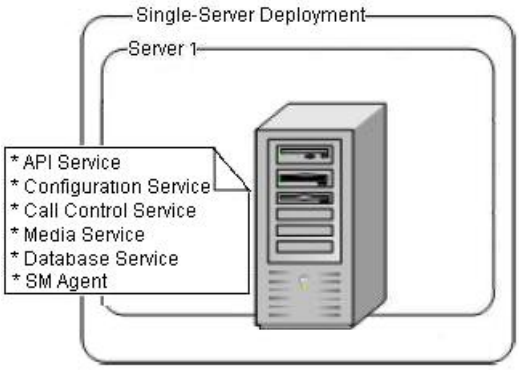
Single-server deployments

A single-server deployment has one MediaSense server on the Unified Communications OS platform. All network services are enabled by default.

In single-server deployments, the primary server has the following feature services:

- API service
- Configuration service
- Call control service
- Media service
- Database service
- SM agent

Figure 1: Cisco MediaSense single-server deployment



Each single-server deployment supports a maximum of 300 simultaneous sessions and a busy-hour call completion (BHCC) rate of 9000 sessions per hour (with each call having a two minute average duration). Single-service deployments enable you to add more servers later to address redundancy issues, to provide high availability, to increase storage capacity, and to increase simultaneous recording capacity.

Dual-server deployments

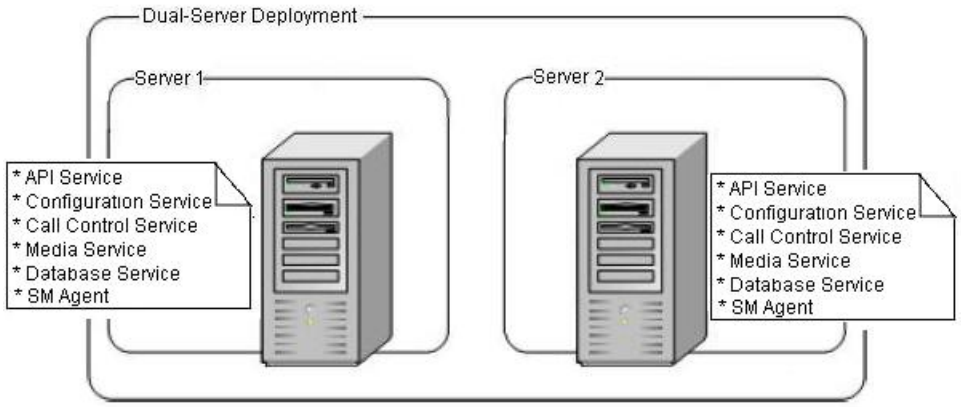
A dual-server deployment has two MediaSense servers on the Unified Communications OS (Unified OS) platform. The first server is called the primary server. The second server is called the secondary server. All network services are enabled on both servers.

Both primary and secondary servers have the following feature services:

- API service
- Configuration service
- Call control service
- Media service
- Database service
- SM agent

Dual-server deployments provide high availability. The recording load is automatically balanced across the primary and secondary servers because all services are always active on both servers.

Figure 2: Dual-server deployment



Note MediaSense does not provide automatic load balancing in the API service or the configuration service. When both of those services are enabled on the primary and secondary servers, you must point your browser or server-based API to *one* of these services.

See the Cisco MediaSense Solution Reference Network Design guide for details about the maximum number of simultaneous recordings, playback, and monitoring sessions that are supported.

Three-server deployments

Three-server deployments have a primary server, a secondary server, and one expansion server. All network services are enabled by default on all servers in the cluster.

The primary server and the secondary server have the following feature services:

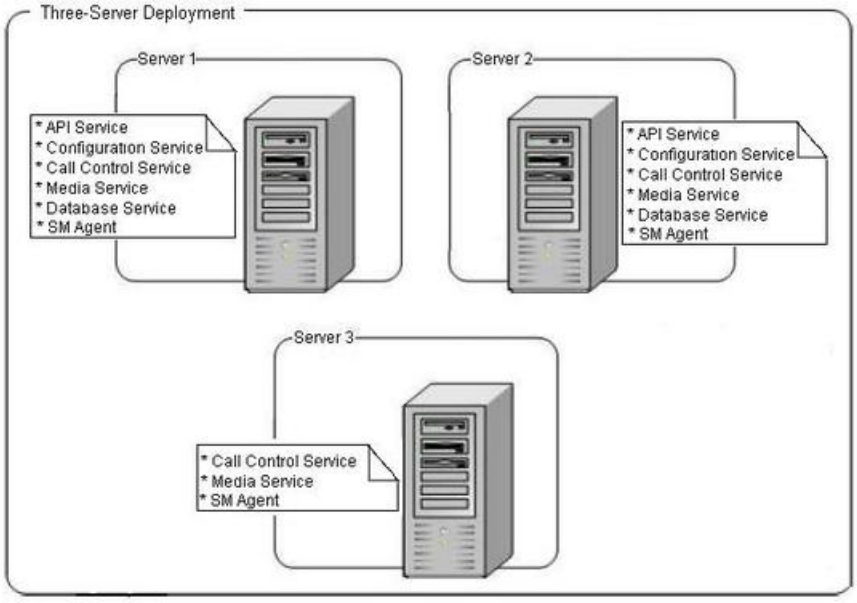
- API service
- Configuration service
- Call control service
- Media service
- Database service
- SM agent

The expansion server has the following feature services:

- Call control service
- Media service
- SM agent

The three-server model provides redundancy and increases storage capacity and simultaneous recording and playback capacity. The recording load is automatically balanced across the servers because services are always active on their respective servers.

Figure 3: Three-server deployment



Note MediaSense does not provide automatic load balancing in the API service and Configuration service on the primary and secondary servers. While those services are enabled, you must point your browser or server-based API to only one of these services.

See the Cisco MediaSense Solution Reference Network Design Guide for details about the maximum number of simultaneous recording sessions, playback sessions, and monitoring sessions that are supported.

Four-server and five-server deployments

Four-server and five-server deployments have one primary server, one secondary server, and two or three expansion servers. All network services are enabled by default on all servers in the cluster.

Primary servers and secondary servers have the following feature services:

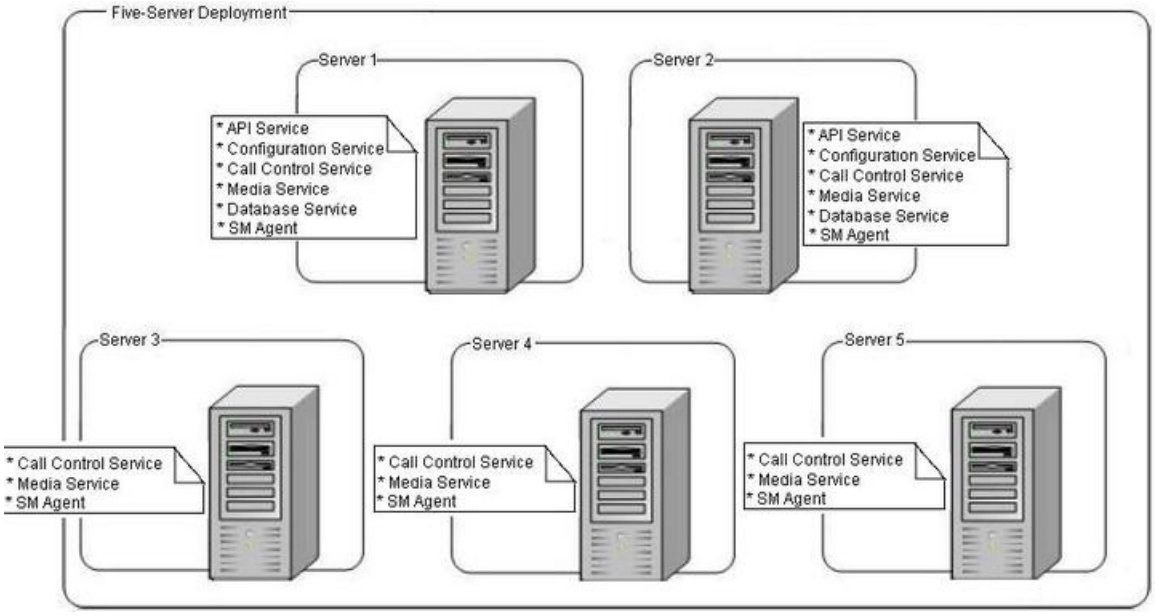
- API service
- Configuration service
- Call control service
- Media service
- Database service
- SM agent

The remaining servers, called *expansion servers*, only have the following feature services:

- Call control service
- Media service
- SM agent

This deployment model provides redundancy, increases storage capacity, and increases capacity for simultaneous recording and playback sessions. The recording load is automatically balanced across the servers because services are always active on their respective servers.

Figure 4: Five-server deployment



Note MediaSense does not provide automatic load balancing in the API service and Configuration service on the primary and secondary servers. While those services are enabled, you must point your browser or server-based API to only one of these services.

See the Cisco MediaSense Solution Reference Network Design Guide for details about the maximum number of simultaneous recording sessions, playback sessions, and monitoring sessions that are supported.

MediaSense high availability deployments

Some deployments require that all available media is recorded. A call control service failure may result in no recordings unless your deployment supports high availability. If Unified CM cannot contact one of the MediaSense servers, you must ensure that an alternate server is available for Unified CM or CUBE to make the required connection.

For more information, see the *Cisco MediaSense Solution Reference Network Design Guide* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html.

Data replication considerations

Database high availability support in MediaSense deployments is provided using Informix enterprise replication (ER) for both the meta database and configuration database. While a MediaSense cluster can have up to five servers, data replication is enabled only between the primary and secondary servers.

At installation time, if the server you are installing is identified as the secondary server, the following considerations apply:

- This server automatically applies the on-tape backup from the primary server without any constraints on the data size in the primary server.
- Data replication is performed between the primary and secondary servers. So data written to the primary server is also replicated to the secondary server, and vice versa.

The replication behavior between the primary and secondary MediaSense servers differs based on the time of replication:

- **Activation time:** During the service activation process, Informix ER automatically begins replication between the primary and secondary servers. The differential data between both servers are replicated from the primary server to the secondary server.
- **Run time:** During run time, data replication is bidirectional. If, for any reason, one of the MediaSense servers is shut down or in a failed state, data continues to be written to the surviving server. When the shut down or failed server is revived, Informix ER automatically restarts between the two servers and synchronizes the data. Depending on the data size, synchronization time may vary. *Retention period* refers to the number of days that data can be stored on the surviving server without breaking the replication. See the Cisco MediaSense Solution Reference Network Design Guide for details about database retention period recommendations.

Data replication and recovery for primary or secondary node

If either the primary or secondary server goes out of service, the database replication process proceeds as follows:

- MediaSense continues to write data to the recording database. Because the data cannot be replicated to the out of service node, Informix stores the data in the ora_ersb replication buffer on the node that is still working. If the node that is out of service comes back up before ora_ersb is full, replication is automatically restored and the data in ora_ersb is synchronized between both nodes.
- If one node is out of service for an extended period, the ora_ersb buffer on the working node may fill up. If ora_ersb reaches 90% of its capacity, the system automatically stops replication on the working node (which then acts like a single node). The system does this to prevent ora_ersb from getting too full and the system from becoming dysfunctional.
- If replication is stopped on the working node, it is automatically restored after the out of service node comes back into service. User intervention is not required. After replication is restored, data sync jobs are launched to compare both the meta data and the configuration data on both nodes and to synchronize this data.

You can check the data sync job status by running the following CLI command on either one of the nodes:

show db_synchronization status [db_ora_meta|db_ora_config]

Deployment considerations for high availability

Follow these guidelines to ensure a high availability deployment and to provide data replication:

- Verify that the API service is enabled and running. The API service monitors its internal performance to provide overload protection. If an overload condition is detected, the API service may begin to automatically reject third-party requests. Client applications should be able to retry requests on the alternate API service if they receive rejections.
- A deployment can contain up to five possible call control services in the cluster.

The following table identifies the possible MediaSense high availability scenarios.

MediaSense scenarios	with Unified CM	with CUBE
Normal scenario	The Unified CM uses a round-robin method to reach an available call control service to place an outbound call and times out if it is still unsuccessful after attempting to reach the last call control service.	CUBE always sends a call to the first MediaSense server in the media-recording list.
Failed server scenario	Unified CM uses the next available MediaSense server in the list.	CUBE uses the next available MediaSense server in the media-recording list.

Failure condition considerations

If a MediaSense primary or secondary server fails for any reason, the surviving server continues to write meta data to the meta database and to the MediaSense Enterprise Replication Smart Binary Large Object. This large object is referred to as the ora_ersb.

If ora_ersb reaches 90% of its capacity, replication on the surviving server stops so that the surviving server can continue to write data. If the ora-ersb exceeds its capacity, the system becomes dysfunctional.

Recovery time is the time taken by the failed MediaSense server to synchronize data with the surviving server after the failed server comes back in service. The length of recovery time for a failed server depends on the following factors:

- the volume of data written to the surviving server when one server is down.
- the duplex network connection speed between the two servers.
- the level of call load running when recovery is in progress.
- whether replication stopped on the surviving server.

A failed MediaSense system can degrade at two levels:

- When ora_ersb is *less than* 90% full. If the failed server is brought back before ora_ersb is 90% full on the surviving server, no metadata is lost.
- When ora_ersb is *more than* 90% full. If the ora_ersb becomes 90% full on the surviving server before the failed server is restored, replication stops on the surviving server. This allows the surviving server to continue to write data so that no metadata is lost. When the failed server comes back into service,

replication must be re-established and it may take longer for services to be ready. It may take substantially longer to synchronize the data after the failed server comes back into service.

In both situations, when the failed server is back up and available, replication automatically starts to catch up. No manual intervention is required.

For details about failure recovery times, see the *Cisco MediaSense Solution Reference Network Design Guide* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html).

MediaSense requirements

This section identifies requirements for MediaSense.

Media storage requirements

Cisco provides an Open Virtualization Archive (OVA) Virtual Machine (VM) template with options for primary and secondary servers, for expansion servers, and for smaller configurations. These template options specify the supported VM configurations for MediaSense servers. These template options specify, among other things, a memory footprint and a requirement for the available CPUs on specifically identified servers. You must use this Cisco-provided template in all of your MediaSense Servers.

To ensure high availability in environments with two or more MediaSense servers, you must install the primary and secondary servers on different physical hosts.

For more information, see the *Cisco MediaSense Solution Reference Network Design Guide* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html.

Hardware requirements

MediaSense is packaged with the Linux-based Unified Communications Operating System (OS), an appliance model developed by Cisco.

An approved servers for MediaSense must meet the following hardware requirements:

- Approved Unified Computing System (Unified CS) servers. For a list of approved UCS servers, see the *Cisco MediaSense Solution Reference Network Design Guide* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html.
- In addition to the approved servers, MediaSense can be installed on a UCS-E modules inside a router. A UCS-E module is a router blade that has its own processors, storage, network interfaces, and memory. For more information about approved UCS-E models, see the *Cisco MediaSense Solution Reference Network Design Guide* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html. For more information about UCS-E modules, see http://www.cisco.com/en/US/products/ps12629/index.html.
- Virtual Machine (VM) requirements specific to MediaSense are available at http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_MediaSense.

  For details about VM templates, ESXi, sizing information, and other VM-specific process details, see http://cisco.com/go/uc-virtualized.

- For more information about hardware limitations. see the *Cisco MediaSense Release Notes* on Cisco.com (CDC) at http://www.cisco.com/en/US/products/ps11389/prod_release_notes_list.html .

Software requirements

MediaSense must meet the following software requirements:

- The required Unified CM cluster must already be configured and deployed before you set up MediaSense.
- The MediaSense administration web interface uses approved web browsers. For a list of approved web browsers, see the *Cisco MediaSense Solution Reference Network Design Guide* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html.

License requirements

The primary licensing and feature activation method for MediaSense is trust-based licensing, therefore you do not need to install any MediaSense licenses.

Other requirements

MediaSense must have an uninterrupted power supply at all times to prevent unpredictable behavior due to power failure.

Port usage

The section identifies the TCP and UDP ports that are used by MediaSense.

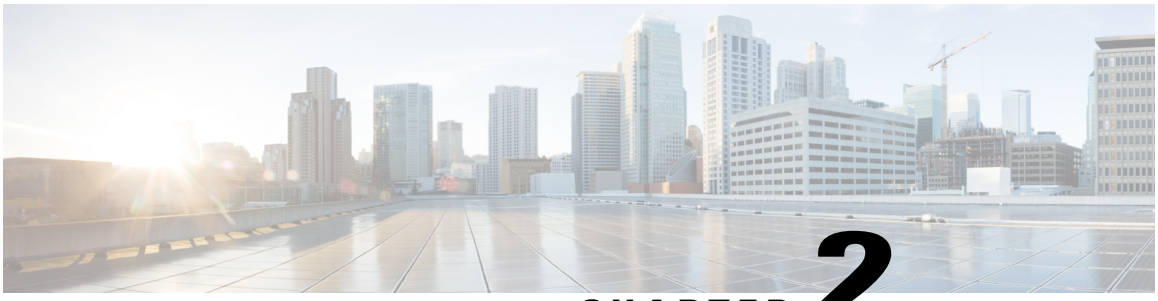
Note Users cannot configure these ports. The table below shows how MediaSense is configured when it is installed.

The columns in the table below provide the following information:

- **Server or application protocol:** the name of the open or private application protocol.
- **Server protocol and port:** the TCP or UDP port that the server or application is listening on, along with the IP address for incoming connection requests when acting as a server.
- **Remote protocol and port:** the TCP or UDP port that the remote service or application is listening on, along with the IP address for incoming connection requests when acting as the server.
- **Remote device:** the remote application or device making a connection to the server or service.
- **Used by:** the service, services, or agents that use each port or ports.

Server or application protocol	Server protocol and port	Remote protocol and port	Remote device	Used by
HTTPS	TCP 443, 8443	Any	Web browser	Administration, serviceability
HTTPS	TCP 8440	Any	Client application	API access
HTTPS	TCP 9443	Any	Client application	Used by media dervice to redirect authenticated requests.
HTTP	TCP 80, 8080	Any	Web browser	Administration, serviceability
HTTP	TCP 8081	Any	Web browser, API client	Call control service
HTTP	TCP 8085	Any	Another CMS node	Call control service
HTTP	TCP 8087	Any	CMS cluster nodes only	System service
HTTP	TCP 8088	Any	CMS cluster nodes only	Configuration service
RTSP	TCP 554, 8554	Any	RTSP media player	SM agent
RTSP	TCP 9554	Any	Client application or media player	Used by media service to redirect authenticated requests.
SIP	TCP 5060 UDP 5060	TCP 5060 UDP 5060	Unified CM or CUBE	Call control service
TCP/IP	TCP 1543	Any	CMS cluster nodes only	Used by Informix ER to make connections between primary server and secondary servers. Used by API service or configuration service to make JDBC connections with Informix.

Server or application protocol	Server protocol and port	Remote protocol and port	Remote device	Used by
Keep-alive heartbeats	UDP 8091	UDP 8091	CMS cluster nodes only	Used by a call control service to detect availability of other call control services.
JMS	TCP 61610	Any	CMS cluster nodes only	API service
JMS	TCP 61612	Any	CMS cluster nodes only	Call control service
JMS	TCP 61616	Any	CMS cluster nodes only	SM agent
Ephemeral port range	UDP 32768 - 61000	Any	Phone or gateway that sends RTP media streams.	Range of ports used by media service to receive RTP media streams.



CHAPTER 2

Install or Upgrade MediaSense

This chapter contains information for installing and upgrading MediaSense.

- Install MediaSense, page 21
- Upgrade MediaSense, page 35
- Rollback cluster, page 41
- Install COP files, page 42
- Language pack, page 43

Install MediaSense

This section describes how to install MediaSense and the Cisco Unified Communications Operating System (Unified OS). You install both with one program.

Pre-installation tasks and tools

Before you start, verify that you are using hardware and software that Cisco supports. For a list of supported hardware and software, see the *Cisco MediaSense Solution Reference Network Design Guide* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html.

Installation and configuration worksheet

Make one copy of this worksheet for every node or server in the cluster. Record the network, password, and other information that the installation and setup wizard prompts you to enter for each server. You may not need to record all the information; record only the information that is pertinent to your system and network configuration.

Store the completed worksheets in a secure location for future reference.

Installation data	Your entry	Notes
Platform administrator information	Username: Password:	Information used to sign in to the Unified Communications Operating System Administration and to Cisco Unified Serviceability.

MediaSense application administrator information	Username:
	Password:
		Information used to sign in to MediaSense administration and serviceability.
		You can change the entry after installation by using the CLI commands:
		`utils reset_application_ui_administrator_name`
		`utils reset_application_ui_administrator_password`

MediaSense cluster deployment information	Primary server IP address: Secondary server IP address: Expansion server IP address(es):	
The MTU size (in bytes) for your network. This setting must be the same on all servers in a cluster.	MTU size:	If you are unsure of the MTU setting for your network, use the default value of 1500 bytes.
Static network configuration	IP Address: IP Mask: Gateway:	
DNS client configuration	Primary DNS: Secondary DNS (optional): Domain:	Provide this information when using hostnames for cluster configuration. A server hostname cannot be changed after installation. If you enable DNS, you must configure both forward and reverse lookup information.
Network Time Protocol (NTP) or hardware clock configuration for the first server. Set the NTP for other servers in the MediaSense deployment to the time on the first server.	Hostname or IP address of the NTP server(s):	You must specify *at least* one valid and reachable NTP server.

Installation data	Your entry	Notes
Enter the same security password for all servers in the MediaSense deployment.	Security password:	The security password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character. You can change the entry after installation by using the CLI command: `set password security`.

Answer files for unattended fresh installations

You can perform an unattended, fresh installation of MediaSense by using a platform configuration file called an answer file. Answer files are created using a Web-based application called the Cisco Unified Communications Answer File Generator.

The Answer File Generator simultaneously validates the syntax of your data entries, saves the data, and generates the platform configuration file.

Use an answer file to create and mount a virtual image of MediaSense on a memory stick or a disk. Use this image to perform an *unattended* installation on the primary node, secondary node, or any expansion nodes in a cluster. You cannot use it to upgrade an installation.

To create an answer file, visit the answer file generation Web site.

For more information, see How to Use the AFG with the Virtual Floppy Drive.

Navigate the installation wizard

Note If you leave an installation unattended, your monitor screen may go blank. If the screen goes blank:

- press **Escape** to redisplay the current screen and continue the installation.
- do *not* press the space bar, as this selects the default option from the current screen and moves you to the next screen.

The following table describes the actions the system takes when you enter certain keys during installation.

To do this...	Press this...
Move to the next field	Tab
Move to the previous field	Alt-Tab
Choose an option	Space bar or Enter
Scroll up or down in a list	Up and Down arrow
Return to the previous window	Space bar or Enter to choose Back (when available)

To do this...	Press this...
Get help for a window	Space bar or Enter

Installation process

The installation process deploys the MediaSense application and the Unified Communications Operating System (Unified OS) from the provided media on the DVD disc.

Before you install the MediaSense, you must address all virtual machine (VM) requirements.

Cisco assumes that you know the VMware tool set and have completed the following tasks:

- Mounted and mapped the DVD drive to the VM host DVD device (physical DVD drive with the DVD disk inserted) or you have mounted your DVD drive to the datastore ISO file.
- Powered on your VM server in preparation for this installation.
- Met all of the VM requirements listed in the **Unified Communications Virtualization** website at http://cisco.com/go/uc-virtualized.

You can install MediaSense from the installation disc and configure it with one DVD insertion. The disc contains the Unified OS and the MediaSense installer. When you run this installer, you install Unified OS and MediaSense at the same time.

Installing MediaSense is a two-step process:

1. Install MediaSense and Unified OS.
2. Setup the primary server.

Note Before you install any secondary or expansion servers, the primary server must be running and it must be configured with information about the secondary and expansion servers.

Install MediaSense and Unified OS

- Use one of the supported VM template options to plan your full configuration. If your plan does not match one of the supported VM template options, MediaSense defaults to unsupported mode and a limited number of recording resources become available. Cisco provides no technical support for systems running in an unsupported mode. To view all VM requirements, visit the Unified Communications Virtualization website at http://cisco.com/go/uc-virtualized.
- Assign the primary and secondary servers. The installation process for the primary server differs from the process for all other servers. After you assign your primary and secondary servers, you cannot change the assignment.
- Place the CD/DVD device at the top of the BIOS boot order.
- If you plan to perform an unattended installation, provide a configuration file on a virtual image.

Caution The installation may fail if an invalid or incorrect IP address was entered when the MediaSense node was added to the Unified CM cluster. Refer to http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Cisco_MediaSense for information on correcting the IP address before restarting the installation.

Caution If a critical error occurs during installation, the installer prompts you to collect log files. You may need to restart the installation of this node. For more detailed instructions, see How to Dump Install Logs to the Serial Port of the Virtual Machine.

Procedure

Step 1 If you have a configuration file for an unattended installation, confirm that it is on a virtual image, that the image is on the datastore, and that it is mounted. For more information, refer to http://docwiki.cisco.com/wiki/How_to_Use_the_AFG_with_the_Virtual_Floppy_Drive.

Step 2 If you are using a MediaSense installation disk, configure the virtual machine to see the physical DVD device on the host. Wait until the **DVD Found** window is displayed.

Step 3 You are prompted to perform a media check. The media check verifies the integrity of the installation disc. If your disc passed the media check previously, omit this step.
To perform a media check, select **Yes**. To omit the media check, select **No** and continue to step 4.

Note During the media check, the **Media Check Result** window displays a progress bar. Depending on your server setup, the media check can take up to an hour to complete.

a) If the Media Check Result displays PASS, click **OK** to continue.
b) If the media check fails, eject the DVD to end the installation. At this point, the next step depends on your service-level agreement. You can:

- Obtain another installation disc directly from Cisco Systems.
- Contact your service provider for assistance.

The **Cisco Unified Communications Product Deployment Selection** screen is displayed.

Step 4 Click **OK** on the **Cisco Unified Communications Product Deployment Selection** screen to proceed.
The installation begins.

Step 5 Select **Yes** if you agree with the information that is displayed in the **Proceed with Install** screen. If you select **No**, the installation is cancelled.
The screen displays any pre-existing version of MediaSense on the hard drive and the version that is available on the disc. For an initial installation of MediaSense, the version on the hard drive is displayed as `NONE`.

If you plan to perform an unattended installation and provided configuration information Step 1 of this procedure, select **Yes** in the **Proceed with install** screen. The installer asks no more questions unless there is a discrepancy in the configuration information. When the installation process is complete, perform the tasks in Post-installation tasks, on page 27.

If you did not provide configuration information in Step 1, and you select **Yes** in the **Proceed with Install** screen, the installation continues with the next step.

Step 6 In the **Platform Installation Wizard** screen, select **Proceed**.
The software installation begins.

Note During the installation process, some system messages prompt you to press a key. **Do not press a key**.

Step 7 When the VM prompts you to eject the DVD, eject the DVD and close the tray.

Step 8 In the **Basic Install** screen, click **Continue** .
The **Setup Configuration** wizard launches and displays a series of screens with options pertinent to your MediaSense deployment.

Step 9 In the **Time Zone Configuration** screen, use the **Up and Down** arrow to select the time zone for your server location. Click **OK**.

Caution Setting the time zone incorrectly can adversely affect system operation.

Step 10 In the **Auto-Negotiation Configuration** screen, select **Continue**.

Step 11 In the **MTU Configuration** screen, select **No** to keep the default setting (1500).
The MTU is the largest packet (in bytes) that this host will transmit on the network. Use the default setting if you are unsure of the MTU setting for your network. If you do not want to use the default setting, contact your network administrator to identify the setting that is required for your deployment.

Caution If you do not configure the MTU size correctly, network performance can be degraded.

Step 12 In the **Static Network Configuration** screen, enter the values for IP Address, IP Mask, and Gateway (GW) Address. Click **OK**.

Step 13 In the **DNS Client Configuration** screen, select **Yes**.

Note
- If you enable DNS, you can use hostnames to configure the nodes. Hostnames cannot be changed after installation completes.
- If you disable DNS, you must use IP addresses to configure the nodes.

If you enable DNS, you must provide values for the **Primary DNS** and the **Domain**. Optional values include the **Secondary DNS**.

Note If you enable DNS, you must also configure both **forward and reverse lookup** information in your DNS server. If you do not configure this information, the installation fails on the network check.

Step 14 In the **Administrator Login Configuration** screen, enter the Administrator ID for the Unified OS (platform) administrator for this deployment. Also enter and confirm the password for this administrator. Select **OK**.

Step 15 In the **Certificate Information** screen, enter values for Organization, Unit, Location, State, and Country. Click **OK**.

Step 16 The next step depends on if you are configuring the first (primary) server or if you are configuring a secondary or expansion server.
If you are configuring the **first (primary)** server for this MediaSense deployment, select **Yes** in the **First Node Configuration** screen.

Caution After you install the primary server you *cannot* change your primary server assignment for this deployment.

a) In the **Complete the Network Time Protocol Client Configuration** screen, enter **NTP Servers** and click **OK**.
The first (primary) server in a MediaSense deployment can get its time from any external Network Time Protocol (NTP) server that you define. NTP or hardware clock configuration is only set for the first node. Other servers in the cluster automatically synchronize their time to the time on the first server.

Note You must specify *at least* one valid and reachable NTP server.

b) Enter the security password in the **Security Configuration** screen.
The security password:

- must start with an alphanumeric character and be at least six characters long. It can contain alphanumeric characters, hyphens, and underscores.
- must be identical for all servers because the servers use it to authorize communications between themselves.
- must be recorded and kept to use again when you add a secondary server or an expansion server.
- can be changed later using the CLI command `set password security`.

Select **OK**.

c) In the **Application User Configuration** screen, enter the user ID for the application user. Enter and confirm the password. Click **OK**.
To complete the installation of the first (primary) server, go to Step 21.

If you are configuring a **secondary** server or an **expansion** server, select **No** and continue to the next step.

Step 17 A warning indicates that if you are configuring a **secondary** or **expansion** server, you must have configured the server on the primary server first, and that the server you are configuring must have access to the primary server.
Select **OK** and proceed to the next step.

The **Network Connectivity Test Configuration** screen appears.

Step 18 Select **Yes** to pause then the installation and add the subsequent server information to the primary server. For instructions, see MediaSense server configuration, on page 30.
Resume the installation after the configuration is complete.

Step 19 In the **First-Node Access Configuration** screen, add the Host Name and IP Address of the first (primary) server. The security password is the same as the security password you entered for the first server. Click **OK** to continue with the installation.
The **Platform Configuration Confirmation** screen is displayed.

Step 20 In the **Platform Configuration Confirmation** screen, select **OK** to proceed with the installation.
The installation process continues. The process may take several hours to complete. Completion time depends on the configuration setup, hardware setup, disk size, and other factors.

MediaSense restarts automatically after the installation completes. A login screen displays a successful installation message and a login prompt.

What to Do Next

Un-mount the DVD drive mapped to the VM host DVD device (physical DVD drive with the DVD disk inserted) or the DVD drive mounted to the datastore ISO file.

Proceed with post-installation tasks to complete the set up for every node in the cluster.

Post-installation tasks

After installing MediaSense on your primary server, you must set some configuration parameters and perform other post-installation tasks before you start using the system.

Procedure

Step 1 Upgrade the VM tools.
For more information on upgrading VM tools, see http://docwiki.cisco.com/wiki/VMware_Tools.

Step 2 Complete the setup of the primary server.
See Complete setup for primary server, on page 28.

Step 3 Add subsequent servers.
See MediaSense server configuration, on page 30.

Step 4 Complete the setup of each subsequent server.
See Finish setup for subsequent servers, on page 31.

Complete setup for primary server

The Unified CM IP address and the Administrative XML Layer (AXL) administrator username and password are required to perform the post-installation setup procedure. Access to Unified CM is required to continue with the MediaSense setup.

Note The AXL user can only be an end user in Unified CM.
For Unified CM 10.0, the AXL user must be configured with the following roles:

- Standard AXL API Access
- Standard CCM Admin Users

For Unified CM 9.1, the AXL user must be configured with the following roles:

- Standard AXL API Access
- Standard CCM Admin Users
- Standard CCMADMIN Administration
- Standard SERVICEABILITY Administration

For more information about Unified CM users and roles, see Cisco Unified Communications System Documentation.

See the following sections to review the considerations for your intended deployment :

- Single-server deployments, on page 10
- Dual-server deployments, on page 11
- Three-server deployments, on page 12
- Four-server and five-server deployments, on page 13

Caution After you install the primary server you *cannot* change your primary server assignment for this deployment.

Follow this procedure to complete the setup for the primary server in any MediaSense deployment.

Procedure

Step 1 After you complete the installation procedure, the system automatically restarts. Sign in to MediaSense Administration for the primary server.
The Welcome screen of the MediaSense First Server Setup wizard is displayed.

Step 2 When you are ready to proceed, click **Next.**
The **Service Activation** screen is displayed.

Step 3 The system internally verifies the IP address of this server and automatically begins enabling the MediaSense feature services in this server. Wait until all the features services show as enabled in the Service Activation window. After all the services are successfully enabled, click **Next.**
If a feature service cannot be enabled, an error message is displayed in the Status section.

Table 2: Feature service status descriptions

Status	Description	Action
Enabling	This service is in the process of being enabled.	Wait for the state to moved to the Enabled.
Enabled	This service is now fully turned on and ready to function.	Wait until all the feature services for this server reach the Enabled state. The primary server requires all feature services to be enabled.
Error	The system cannot enable this service due to an error.	**Warning** If the Database service or the feature services are not enabled, the system will not allow you to proceed with the setup procedure. Your response depends on the service that failed to be enabled. • If it is the database service or the configuration service that failed, you must first correct the error and restart the initial setup. • If it is any other service that failed, you can continue with the setup and fix the errors after the setup is completed. Be aware that your system will not be fully in service until you fix these issues.

After you click Next, the **AXL Service Provider** screen appears.

Step 4 Enter the AXL service provider (IP address) and the AXL administrator username and password in the respective fields for the Unified CM that should communicate with MediaSense.

Note You will not be able to change the password for the AXL user in the MediaSense application. The MediaSense application only authenticates the password configured in Unified CM. You can, however, modify the AXL server IP address. See Select AXL service providers, on page 47.

If the selected AXL services cannot be enabled, an error message instructs you to reselect AXL service providers.

After the system accepts the AXL server and user information, the **Call Control Service Provider** screen appears.

Step 5 If the client applications using MediaSense need to make outbound recording calls, provide the Unified CM server IP address for the call control service on the **Call Control Service Provider** screen.

Note Provide this information only if you know the applications using MediaSense. You can get this information by sending an AXL request to the Unified CM server that was configured as the AXL Service Provider.

Step 6 Click **Finish** to complete the initial setup for the primary server.
The **MediaSense Setup Summary** window displays the result of the initial setup.

You have now completed the initial setup of the primary server for MediaSense.

Step 7 In Unified CM Administration, configure the SIP trunk, route group, route list, and recording profile. When you finish the post-installation process for any MediaSense server, you must access the Unified CM server for your deployment (based on the information provided during the installation and post-installation process). For more information, see Set up call control service connection, on page 33.

Step 8 Before you install MediaSense on a secondary server or an expansion server, you must configure details for these servers on the primary server. You configure details for these servers using the MediaSense Administration user interface. For more information, see MediaSense server configuration, on page 30.

MediaSense server configuration

Procedure

Step 1 From the **Cisco MediaSense Administration** menu, select **System** > **MediaSense Server Configuration**.

Step 2 In the **MediaSense Server Configuration** screen, click **Add MediaSense Server**.
The **Add MediaSense Server** screen in the primary node opens.

Step 3 If your installation uses DNS, enter the hostname of the server that you want to add. If your installation does not use DNS, enter the IP address of the server that you want to add.

Step 4 (Optional) Enter the description of the server that you want to add.

Step 5 (Optional) Enter the MAC address of the server that you want to add.

Step 6 Click **Save**.

Step 7 MediaSense displays a confirmation message near the top of the screen.

You see the configuration details of the server that you added in the **MediaSense Server List**. Note that the server type is "UNKNOWN" at this stage of the installation.

Details for secondary and expansion servers

After you have configured details for the secondary server or expansion server on the primary server, install the secondary server or expansion server to complete the clustering process following the procedure Installation process, on page 24.

Note If you have ever increased the size of the /uploadedMedia partition on your system, after you install a new node, you will need to increase the size of the partition on the new node as well or you may encounter errors when uploaded files propagate to the new node. For more information, see Media partition management.

Finish setup for subsequent servers

The Unified CM IP address and the Administrative XML Layer (AXL) administrator username and password are required to perform the post-installation setup procedure. Access to Unified CM is required to continue with the MediaSense setup.

See the following sections to review the considerations for your intended deployment :

- Single-server deployments, on page 10
- Dual-server deployments, on page 11
- Three-server deployments, on page 12
- Four-server and five-server deployments, on page 13

Caution After you complete the following procedure for the secondary server, you *cannot* change your secondary server assignment for this deployment.

Use the MediaSense Administration interface to make changes to the information that you specify during the setup procedure. For more information, see Administer and Configure MediaSense, on page 45.

Procedure

Step 1 After you complete the installation procedure specified in Install MediaSense and Unified OS, the system restarts automatically and you must sign in to MediaSense Administration to install subsequent servers. When you sign in, the **Welcome** screen of the MediaSense Subsequent Server Setup wizard appears.

Step 2 When you are ready to proceed, click **Next.**

You determine the type of server in this Welcome screen. You must decide whether this subsequent server becomes the secondary server or an expansion server. Based on your choice, the list of services to be turned on is displayed on the service activation page.

- **Secondary server:** enable all of the services in the **Service Activation** window to make this server the secondary server. After you have enabled all the services and the initial setup completes, you *cannot* change the secondary server assignment.

  Once a secondary server has been selected, any additional servers will automatically be designated as expansion servers.

- **Expansion servers:** only the media service, call control service, and SM Agent are enabled on expansion servers. The API service and the configuration service are not available on expansion servers.

The following table shows which features can be enabled in each type of server:

Feature	Enabled in primary server?	Enabled in secondary server?	Enabled in expansion servers?
Database service	Yes	Yes	No
Configuration service	Yes	Yes	No
API service	Yes	Yes	No
Media service	Yes	Yes	Yes
Call control service	Yes	Yes	Yes
SM Agent	Yes	Yes	Yes

Select the server type and click **Next**. The **Service Activation** screen is displayed.

Step 3 After the services are enabled, click **Finish** to complete the initial setup for a subsequent server. If a feature service cannot be enabled, an error message is displayed in the Status section.

The **MediaSense Setup Summary** window displays the result of the initial setup and MediaSense restarts.

You have now completed the initial setup of a subsequent server. This subsequent server is ready to record.

Repeat this setup procedure for each expansion server in the cluster.

System verification

After you install MediaSense, use the following indicators to verify the health of your deployment:

- Sign in to MediaSense Administration on each server. See Access MediaSense Administration, on page 45.
- Sign in to MediaSense Serviceability Administration on each server. See Access MediaSense Serviceability, on page 75.

- Services described in *Setup Summary* are enabled on each server. For status descriptions, see Complete setup for primary server, on page 28.

Unified CM provisioning for MediaSense

When you finish the post-installation process for any MediaSense server, you must access the Unified CM server for your deployment (based on the information provided during the installation and post-installation process).

Perform the following tasks after you finish your cluster setup and before you start using the MediaSense servers.

Set up call control service connection

The call control service in MediaSense is referred to as a SIP trunk in the Unified CM interface and documentation. In Unified CM Administration, you must configure the SIP trunk, route group, route list, and recording profile to enable the call control service in MediaSense Administration to communicate with Unified CM Administration.

Note Be sure to configure Unified CM to use TCP transport for a SIP trunk connection to MediaSense that is active on all call manager nodes.

After you have configured the SIP trunk information in Unified CM, you will need to provide this IP address in the Call Control Service Provider Configuration panel of the **Unified CM Configuration** screen in MediaSense Administration.

Even if already enabled, the call control service will not be *In service* until you have configured the call control service provider.

Use this procedure to configure the SIP trunk information in Unified CM if your installation calls for Built-in-Bridge (BiB) recording.

Procedure

Step 1 Invoke and connect to the Unified CM Administration web interface using a valid Unified CM username and password.

Step 2 If MediaSense is a single-node cluster, skip to the next step. If MediaSense is a multiple-node cluster, select **Device** > **Device Settings** > **SIP Profile** in Unified CM Administration.
Follow the procedure specified in your Unified CM Administration documentation to enable “OPTIONS Ping” and save this configuration.

a) Add a new SIP profile.
b) Select the **Enable OPTIONS Ping** check box to monitor the destination status for SIP trunks using the *None* (default) Service Type.

Step 3 Select **Device** > **Trunk** in Unified CM Administration.
Follow the procedure specified in your Unified CM Administration documentation to add a new SIP Trunk.
To configure the device

- edit the Device Name

- select the Device Pool
- assign SIP information
- enter the destination IP address and port (5060) for MediaSense
- select the SIP trunk security profiles and SIP profile (created in Step 2)
- ensure that the **Media Termination Point Required** checkbox is unchecked
- near the bottom of the screen, select the **Run On All Active Unified CM Nodes** checkbox.

Save this configuration.

You must create one SIP trunk for each server in the MediaSense deployment.

Step 4 Add a new route group by selecting **Call Routing** > **Route/Hunt** > **Route Group** in Unified CM Administration. Set the distribution algorithm to *circular*.
Follow the procedure specified in your Unified CM Administration documentation to select the circular distribution algorithm.

Select all the MediaSense SIP trunks created in Step 3.

Step 5 Create a route list by selecting **Call Routing** > **Route/Hunt** > **Route List** in Unified CM Administration.
Follow the procedure specified in your Unified CM Administration documentation to associate the route list with the route group created in Step 4.

Step 6 Create a route pattern by selecting **Call Routing** > **Route/Hunt** > **Route Pattern** in Unified CM Administration.
From the Gateway/Route List drop-down list under the newly created route pattern page, select the name of the route list configured in Step 5.

Caution Do not include any wildcard characters when creating route patterns for the recording profile.

Step 7 Select **Device** > **Device Settings** > **Recording Profile** in Unified CM Administration.
Follow the procedure specified in your Unified CM Administration documentation to add a new recording profile. Configure the recording profile name, and the recording destination address (enter the route pattern number you configured in Step 6, and click **Save.**

Step 8 Select **Device** > **Phone** in Unified CM Administration.
Follow the procedure specified in your Unified CM Administration documentation to perform the following tasks:

a) Find the audio forking phone.
b) Find the Built In Bridge configuration for this device and change the setting to **ON.**
c) Access the Directory Number Configuration page for the line to be recorded.
d) If you are using a recording partner, select either **Automatic Call Recording Enabled** or **Application Invoked Call Recording Enabled** in the **Recording Option** drop-down list, according to the recording partner recommendations. If you are not using a recording partner, select **Automatic Call Recording Enabled**.
e) Select the recording profile created earlier in this procedure.

Disable iLBC and iSAC for recording device

Caution MediaSense does not support internet Low Bit Rate Codec (iLBC) or internet Speech Audio Codec (iSAC). Consequently, you must disable these features in Unified CM before you proceed with the MediaSense configuration.

Procedure

Step 1 Invoke and connect to the Unified CM Administration web interface using a valid Unified CM username and password.

Step 2 Select **System** > **Service parameters** in the Unified CM Administration.

Step 3 On the **Service Parameter Configuration** web page, select the required server and service (Cisco CallManager) from the **Select Server and Service** drop-down lists.

Step 4 Go to the Cluster-wide Parameters (Location and Region) section and locate the **iLBC Codec Enabled** parameter and the **iSAC Codec Enabled** parameter.

Step 5 Set the value for both of these parameters as *Enable for All Devices Except Recording-Enabled Devices* and save your configuration.

Upgrade MediaSense

This section contains information on how to upgrade MediaSense. MediaSense can only be upgraded from one release to the next supported release. If you are running a an earlier release, you may have to upgrade more than once to bring your system up to the current release.

Each successive release contains minor changes to the MediaSense API that are always upward compatible—with one exception. The exception is between release 8.5(4) and 9.0(1), in which security enhancements were introduced. Those enhancements require that client software be modified in order to provide HTTP-BASIC credentials and to handle a 302 redirect. HTTP-BASIC credentials must now be provided with all RTSP and HTTP download requests.

If an upgrade does not complete, you can rollback to the previous release and begin the upgrade again.

Note A node can take several hours to upgrade depending on the number and size of recordings it holds. Ensure that you are prepared to wait several hours to complete the upgrade.

Upgrade considerations

Keep the following points in mind when you consider a MediaSense upgrade:

- **Full loads—**You cannot run a full call load until after you complete the upgrade on all servers in the cluster.

- **Upgrade sequence—**When you upgrade a cluster, you must upgrade the primary server first. You can upgrade the remaining nodes one at a time or upgrade them all at the same time.
- **VM snapshots—**You must take a VM snapshot of each node before you begin the upgrade. If an error stops the upgrade process, you can restore these VM snapshots to roll back the nodes to their previous states.
  - You do not need to stop each node to take its VM snapshot.
  - You must delete the VM snapshot from each node after the upgrade. MediaSense should not run on a node with a VM snapshot for more than a few days.
- **Temporary outages—**You experience a temporary server outage while the software is being upgraded. How long this outage lasts depends on your configuration and the size of the data that is stored in the database.
- **Aborted calls—**Nodes in the MediaSense cluster stop taking new calls and API requests when you begin the upgrade process. If any calls are in progress when you begin the upgrade, recordings of those calls end in a CLOSED_ERROR state. After the upgrade, each node in the cluster resumes accepting calls when it come back online.
- **Incomplete upgrades—**If you decide to back out of an upgrade before it completes, you must restore the VM snapshots on all nodes in the cluster to their previous version.
- **Potential data loss—**During the upgrade process, do not make any configuration changes to any server. After all nodes have been upgraded and returned to service, you can resume making configuration changes. However, even then, if you need to roll back the upgrade, you will lose these configuration changes.

Note To avoid the potential loss of configuration changes or recording data, upgrade only when the cluster is idle.

- **Restarting an upgrade on a subsequent server—**If an upgrade on a subsequent server fails, correct the errors which caused the upgrade failure. Verify the network connectivity of the servers in your cluster. Restore the snapshot on the subsequent server and ensure that its memory and CPU usage are not too high. Upgrade the subsequent server again.
- **COP file installation—**Users are reminded to install any required COP files (including the language pack COP) after each upgrade.

Key points when upgrading from previous releases

A new VMWare VM template was provided in release 9.1(1) that provisions 16 GB of memory rather than the 8 GB that was called for in release 9.0(1) and earlier. For any server being upgraded to or through release 9.1(1), the VM configuration must be manually adjusted to reserve this increased amount of memory.

A new feature was added in release 9.1(1) that permits recorded media storage to be increased in size after installation. However, this feature is not available in systems upgraded from prior releases; it only functions in systems that have been fresh-installed with release 9.1(1) or 10.0(1), or systems upgraded to release 10.0(1) from 9.1(1). The new uploaded media partition is automatically created during upgrade and does support the capability to be increased in size after installation.

If you upgrade a MediaSense cluster from 9.0(1) to 9.1(1) or 10.0(1) and then wish to add nodes to your cluster, be aware that although the new nodes will be installed with expandable recorded media storage, Cisco

does not support that flexibility. Provision approximately the same amount of recording space on each new node as is available on each upgraded node. Although storage space disparity across nodes in the cluster does not present a problem for MediaSense, it could result in pruning ahead of the configured retention period on smaller nodes. Administrators may find this behavior unpredictable.

Upgrade cluster to release 10.0(1)

This procedure describes a cluster where one or more individual nodes (servers) are upgraded. To upgrade individual nodes, see Node upgrade procedures, on page 38.

Note For release 10.0(1), MediaSense no longer supports Vmware ESXi 4.0 and 4.1. Customers must upgrade their hosts to ESXi 5.0 or 5.1 before they can upgrade to MediaSense release 10.0(1).

If you are running an earlier release of MediaSense, you must upgrade to release 9.1(1) before you can upgrade to release 10.0(1). Refer to the *Cisco MediaSense User Guide* for release 9.1(1) at http://www.cisco.com/en/US/products/ps11389/products_user_guide_list.html to upgrade to release 9.1(1) before using the procedure in this document to upgrade to release 10.0(1).

Before you upgrade the cluster, you may want to review some of the following information sources:

- For information about supported upgrades, see the *Cisco MediaSense Solution Reference Network Design Guide* at http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html.
- For information about VM Snapshots, see the VMware documentation.

When you upgrade a cluster:

- You do not need to stop each node to take its VM snapshot.
- You can upgrade the expansion nodes one at a time or upgrade them all at the same time.

Note After you begin the upgrade process on a given node, you cannot cancel it using the Cancel button that appears on some screens. The proper way to cancel the upgrade on a particular node is to restore its VM snapshot.

Procedure

Step 1 Take a VM snapshot of each node.

Step 2 Upgrade the primary node and wait for it to restart. (See Node upgrade procedures, on page 38.)

Step 3 Upgrade the secondary node (if applicable) and wait for it to restart.

Step 4 Upgrade all expansion nodes (if applicable) and wait for them to restart.

Step 5 Upgrade the virtual hardware of each node by selecting "Upgrade virtual hardware" in the vSphere client.

Step 6 Once all of the nodes have been successfully upgraded, delete the VM snapshot on each node.

Node upgrade procedures

This section provides procedures for upgrading nodes using software from

- a local source
- remote sources using either
  - the command line interface (CLI)
  - or Unified OS Administration.

Upgrade nodes from a local source

Note Before you begin this procedure, be aware that just copying the .iso file to the DVD in the first step will not work. Most commercial disk burning applications can create ISO image disks.

Procedure

Step 1 If you do not have a Cisco-provided upgrade disk, create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.

Step 2 Insert the new DVD into the physical DVD device on the host and configure your virtual machine to use that device.

Step 3 Sign in to the web interface for the Unified OS Administration.

Step 4 Navigate to **Software Upgrades** > **Install/Upgrade**.
The **Software Installation/Upgrade** window appears.

Step 5 From the list, choose **DVD**.

Step 6 Enter a slash (/) in the Directory field.

Step 7 Click **Next**.

Step 8 Choose the upgrade version that you want to install and click **Next**.

Step 9 In the next window, monitor the progress of the download.
MediaSense automatically

- upgrades to the release specified
- switches versions and reboots
- starts taking calls.

Remote sources

Note

Cisco certifies certain SFTP products through the Cisco Developer Network (CDN).

CDN partners certify their products with specified versions of Cisco Unified Communications Manager. See GlobalSCAPE (http://www.globalscape.com/gsftps/cisco.aspx) for more information. For issues with third-party products that have not been certified through the CDN process, contact the corresponding third-party vendor for support.

Cisco does not support using the free FTDP SFTP product because of the 1GB file size limit on this product.

Cisco uses the following servers for internal testing. You may use one of these servers, but you must contact the vendor directly for support:

- Open SSH: (http://sshwindows.sourceforge.net)
- Cygwin: (http://www.cygwin.com)
- Titan: (http://www.titanftp.com)

You can upgrade nodes from a remote source using one of two methods:

- Upgrade nodes using Unified OS Administration, on page 39
- Upgrade nodes using Unified OS CLI, on page 40

Upgrade nodes using Unified OS Administration

Note You can also use the Unified OS command line interface (CLI) to upgrade a node from a network location or to upgrade a node from a remote server. For instructions, see Upgrade nodes using Unified OS CLI, on page 40.

Procedure

Step 1 Put the upgrade file on an FTP server or SFTP server that the node that you are upgrading can access.

Step 2 Sign in to the web interface for Unified OS Administration.

Step 3 Navigate to **Software Upgrades** > **Install/Upgrade**. The **Software Installation/Upgrade** window is displayed.

Step 4 From the list, choose **Remote Filesystem**.

Step 5 In the Directory field, enter the path to the directory that contains the patch file on the remote system. If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path.
For example, if the upgrade file is in the patches directory, enter `/patches`

If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including the following:

- Begin the path with a forward slash (/) and use forward slashes throughout the path.

- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path (for example, C:).

Step 6 In the Server field, enter the server name or IP address.

Step 7 In the User Name field, enter your user name on the remote server.

Step 8 In the User Password field, enter your password on the remote server.

Step 9 Select the transfer protocol from the Transfer Protocol field.

Step 10 To continue the upgrade process, click **Next.**
The option to "Switch to new version after upgrade" may safely be ignored.

Step 11 Choose the upgrade version that you want to install and click **Next.**

Note If you lose your connection with the server or close your browser during the upgrade process, you may see the following message when you try to access the Software Upgrades menu again.

Warning Another session is installing software, click **Assume Control** to take over the installation. If you are sure you want to take over the session, click **Assume Control**. If Assume Control does not display, you can also monitor the upgrade with the Real Time Monitoring Tool.

Step 12 In the next window, monitor the progress of the download.
MediaSense automatically

- upgrades to the release specified
- switches versions and reboots
- starts taking calls.

Upgrade nodes using Unified OS CLI

Note You can also use the web interface of the Unified OS Administration to upgrade a node from a network location or to upgrade a node from a remote server. For instructions, see Upgrade nodes using Unified OS Administration, on page 39.

Procedure

Step 1 Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.

Step 2 Sign in to the Unified OS console. See CLI access, on page 104 for more information.

Step 3 Enter `utils system upgrade initiate` at the CLI prompt.
The following options display in the console:

- 1) Remote Filesystem Via SFTP
- 2) Remote Filesystem Via FTP
- 3) DVD/CD

- q) quit

Step 4 Enter **1** or **2** to select the remote file system containing your upgrade file.

Step 5 Enter the path to the directory that contains the upgrade file on the remote system. If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path.
For example, if the upgrade file is in the patches directory, enter `/patches`

If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including the following:

- Begin the path with a forward slash (/) and use forward slashes throughout the path
- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path (for example, C:).

Step 6 Enter the server name or IP address.

Step 7 Enter your user name on the remote server.

Step 8 Enter your password on the remote server.

Step 9 Enter the SMTP host server or press Enter to continue.

Step 10 Select the transfer protocol.

Step 11 Choose the upgrade version that you want to install and press **Enter**.

Step 12 Answer **Yes** to the prompt to start the installation.

Step 13 Monitor the progress of the download.
MediaSense automatically

- upgrades to the release specified
- switches versions and reboots
- starts taking calls.

Rollback cluster

All nodes in a MediaSense cluster must run the same software version. If an upgrade fails, restore the VM snapshots on the nodes to roll the software back to a previous version. After you rollback the software on the nodes in a cluster, you lose all recordings, all configuration changes, and all metadata changes that were made after the upgrade. You regain all recordings that were deleted after the upgrade.

MediaSense clusters cannot run a full call load until you complete the final step in this rollback procedure.

Note Be sure that you use MediaSense Serviceability Administration to perform this procedure. Do not use Unified Serviceability Administration. You can find MediaSense Serviceability Administration in the **Navigation** drop-down menu.

Procedure

Step 1 Stop all nodes in the cluster.

Step 2 Restore and delete the VM snapshots from all nodes in the cluster.

Step 3 Using a Web browser, sign into MediaSense Serviceability Administration.

Step 4 Restart the primary node and wait for it to come back into service.

Step 5 Restart the remaining nodes either one at a time or all together.
After each node comes back into service, it begins taking calls again.

Install COP files

The Cisco Options Package (COP) file provides a generic method to deploy Cisco software outside the normal upgrade process. You can use a COP file to install new language packs, patch fixes, and virtualization tools. You must download and save the COP file before you install it on the nodes in a MediaSense cluster.

The procedure for installing a COP file on a node is the same as the procedure for upgrading MediaSense on that node, but you download a COP file instead of downloading an upgrade (ISO) file.

COP files can generally be installed on an active, running system in a shorter time frame than an upgrade file. However, unlike upgrades, COP files cannot be removed or rolled back.

The following guidelines apply to installing COP files:

- Install the COP file on every node (server) in a MediaSense cluster.
- Restart each node after you install a COP file on it.

Note This procedure provides general guidelines for installing COP files. Before you use this procedure, check the Readme file for the specific COP file that you want to install. If the instructions in the Readme file differ from these general guidelines, follow the instructions in the Readme file instead.

Procedure

Step 1 Go to the MediaSense Download Software Website at http://www.cisco.com/cisco/software/type.html?mdfid=283613140&catid=null.

Step 2 Download and save the MediaSense COP file to a local source or to an SFTP server that can be accessed by the MediaSense server.

Step 3 If you downloaded and saved the COP file to a local source, follow the instructions in Upgrade nodes from a local source, on page 38. (Remember to replace the upgrade filename with the COP filename.)

Step 4 If you downloaded and saved the file to an SFTP server, follow the instructions in Remote sources, on page 39. (Remember to replace the upgrade filename with the COP filename.)

Step 5 After you install the COP file on all nodes in the cluster, go to the web interface for Cisco Unified OS Administration. To verify the COP file installation, navigate to **Show** > **Software**.

The **Software Packages** window displays the installed Partition Version and the additionally Installed Software Options with its corresponding status.

Language pack

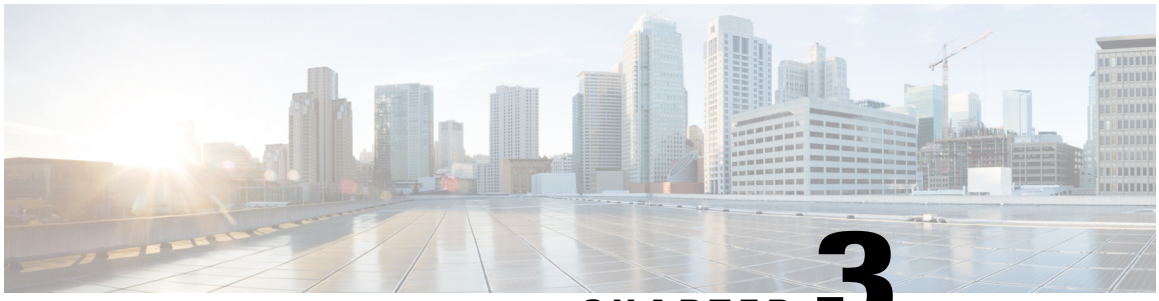
Download and install a language pack only if you want to see the MediaSense interface in a language other than English.

The language pack for MediaSense is delivered as a single cop file, the same way that MediaSense delivers COP files for patches. The files is available to download from Cisco.com and contains a single installer for all language variants. The filename is of the format:

ora-language-pack_18-10.0.1.10000-x.cop.sgn

where *10.0.1* is the release identifier.

Follow the instructions in Install COP files, on page 42 to install the language you want on your interface.



CHAPTER 3

Administer and Configure MediaSense

The MediaSense Administration interface allows you to administer and configure the MediaSense system. You can use a web browser located on any computer on the Unified Communications network to configure and administer your applications with the MediaSense Administration web interface pages.

- Access MediaSense Administration, page 45
- Single sign-in, page 46
- MediaSense Administration , page 46
- Access MediaSense Serviceability, page 75
- MediaSense Serviceability, page 75
- Server IP address changes, page 94
- MediaSense command line interface (CLI) commands, page 104
- Utils commands, page 105
- Run commands, page 107
- Set network commands, page 108
- Show commands, page 110

Access MediaSense Administration

To access MediaSense Administration, you need the application administrator user ID and case-sensitive password that were defined when you installed MediaSense. (If unsure, check your installation and configuration worksheet.) These credentials must be the same for all servers in the cluster.

Procedure

Step 1 From a web browser on any computer in your Unified Communications network, go to `http://Server IP/oraadmin`.
The *Server IP* is the IP address of the server on which you installed MediaSense.

Step 2 A Security Alert message may appear, prompting you to accept the self-signed security certificate. This certificate is required for a secure connection to the server. Click the required button.
This security message may not appear if you have already installed a security certificate.

The MediaSense Administration Authentication page appears.

Step 3 Enter the application administrator user ID and password for the server. Click **Log in**.
The welcome page appears and displays the MediaSense version number, as well as trademark, copyright, and encryption information.

Single sign-in

The Navigation drop-down box in the top right corner of each Administration interface provides a list of applications or pages which you can access with a single sign-in. After you sign in to MediaSense Administration, you can access the following applications:

- **Cisco MediaSense Administration** Used to configure Unified CM, MediaSense users, prune policy, and to perform other tasks described in this section.
- **Cisco MediaSense Serviceability** Used to configure trace files and to enable and disable MediaSense services.
- **Cisco Unified Serviceability** Used to configure trace files and alarms and enable and disable Cisco Unified Communications services. You must be an end user on the configured Unified CM with Administrator privileges for MediaSense to sign into this application.
- **Cisco Unified OS Administration** Used to configure and administer the Cisco Unified Communications platform for MediaSense.

Caution Cisco Unified OS Administration requires a separate (Unified CM) authentication procedure. You must be an end user on the configured Unified CM with Administrator privileges for MediaSense to sign into this application.

To access these pages from MediaSense Administration, select the required application from the Navigation drop-down list and click **Go.**

All MediaSense Administration pages provide descriptive tool tips for each parameter and field. When you place your mouse over the required parameter or field, the tip is briefly displayed for each element.

This document focuses on the functions and services accessed from the **Cisco MediaSense Administration** and **Cisco MediaSense Serviceability** pages. When actions are required on the **Cisco Unified Serviceability** and **Cisco Unified OS Administration** pages, it is clearly identified where to perform these actions.

The minimum supported screen resolution specifies 1024x768. Devices with lower screen resolutions may not display the applications correctly.

MediaSense Administration

The MediaSense Administration menu bar on the left side of the screen contains the following menu options:

- **Administration—**Contains options for configuring new servers in the cluster, Unified CM information, and changing system parameters.
- **System—**Allows you to add a new server or view the disk usage information for each server in the MediaSense deployment.
- **Help—**Provides access to online help for MediaSense.
  - To display documentation for the active administration interface window, click **Help** > **This Page** .
  - To verify the version of the administration running on the server, click **Help** > **About** or click the **About** link in the upper-right corner of the window.
  - To view the latest version of all documents for this release, click **Help** > **Cisco.com**.

    If you are connected to the external network, this link connects you to the home page for Cisco MediaSense.
  - To view the latest version of the troubleshooting tips for this release, click **Help** > **Troubleshooting Tips** .

    If you are connected to the external network, this link connects you to the Trouble Shooting page for Cisco MediaSense.

Unified CM configuration

The topics in the section pertain to a Unified CM cluster and assume that the user has both Unified CM and MediaSense administrator privileges.

Unified CM user information and MediaSense setup

When you access MediaSense Administration for the first time for a given cluster, the system automatically initiates the cluster setup procedure that is described in the Post-installation tasks section.

Select AXL service providers

During the MediaSense post-installation setup process, you may have provided the AXL information for the primary server. If you did not provide this information during the post-installation process or if you need to modify the AXL information, you can do so by following the procedure provided in this section.

Based on the primary server information, MediaSense Administration retrieves the list of other Unified Communications Manager servers in the cluster and displays them in the list of *available* Unified Communications Manager servers. You can select the required server (or servers) and change the Administrative XML Layer (AXL) user information.

Note The AXL service must be enabled for the required Unified Communications Manager server (or servers) before MediaSense Administration can access that server to update the AXL user information.

To modify the AXL information for MediaSense, complete the following procedure.

Procedure

Step 1 From MediaSense Administration, select **Administration** > **Unified CM Configuration**.
The Unified CM Configuration web page opens.

Step 2 In the Unified CM Configuration web page, go to the AXL Service Provider Configuration section to modify the AXL information.
The Unified CM username and password information are mandatory fields. The password cannot be updated on this page. You will need to change the password in Unified CM administration.

Step 3 Select and move each server from the **Available Unified CM Servers** list to the **Selected Unified CM Servers** list box using the right arrow. Alternately, use the left arrow to move a selected server back.

Note When selecting a Unified CM server, ensure that the server you select is a valid Unified CM call control server. The servers in the "Available" list may include Cisco Unified Presence servers as well as Unified CM servers. The Unified Presence servers must not be selected for this purpose.

Step 4 Click the **Save** icon at the top of the Unified CM Configuration web page to save your changes.
The MediaSense server validates the connection details and refreshes the Unified CM Configuration web page to display the new settings.

Select call control service providers

During the MediaSense installation process, you provided the information for the first Unified Communications Manager server. Based on the primary server information, MediaSense retrieves the list of other Unified Communications Manager servers in the cluster and displays them in the list of *available* Unified Communications Manager servers. You can select the required server so that the MediaSense call control service can determine the Unified Communications Manager server to which the outbound call must be sent. If you select multiple Unified Communications Manager servers, you ensure that the outbound call is placed even if one of the servers is not functional.

To modify the call control service information for MediaSense, complete the following procedure.

Procedure

Step 1 From MediaSense Administration, select **Administration** > **Unified CM Configuration**.
The Cisco Unified CM Configuration web page opens.

Step 2 In the Unified CM Configuration web page, go to the Call Control Service Provider Configuration section to modify the call control service provider information.

Note If you deselect the Unified CM server from the Selected list box, a browser window pops up informing you about the deselected servers.

Caution If you modify the Unified CM cluster and do not select the required call control service providers for the new Unified CM server, the MediaSense call control service will be out of service (OOS) and outbound call recording will be disabled.

Step 3 Click the **Save** icon at the top of the Cisco Unified CM Configuration web page to save your changes.
The Unified CM Configuration web page refreshes to display the new settings.

Replace Unified CM service providers

In the Unified CM Configuration web page, you can select Unified CM servers from the available list. However, you cannot modify the IP address for a selected service provider.

To modify the IP addresses that show up in the Available list, you must first add a new AXL service provider.

Caution If you modify the Unified CM cluster configuration, you must also reconfigure the MediaSense API users. If you do not reconfigure the corresponding users, you will not be able to sign in to use your MediaSense APIs.

To replace the Unified CM service provider, complete the following procedure.

Procedure

Step 1 From MediaSense Administration, select **Administration** > **Unified CM Configuration**.
The Unified CM Configuration web page opens.

Step 2 In the Unified CM Configuration web page, click **Modify** Unified CM Cluster to replace the existing list of service providers.
The Modifying Unified CM Cluster web page opens.

Step 3 Enter the IP address, username, and password for the new service provider in the required Unified CM cluster. If you change your mind about this new server, click **Reset** to go back to the Unified CM Configuration web page without making any changes.

Step 4 Click the **Save** icon at the top of the Add New AXL Service Provider web page to save your changes.
The initial list of selected AXL service providers on the Unified CM Configuration web page will be replaced with the selected Unified CM service provider.

The MediaSense server validates the connection details, closes the Modifying Unified CM Cluster web page, and refreshes the Unified CM Configuration web page to display the new service provider in the Selected service provider list. The selected service provider is also updated in the MediaSense database.

Even if you provide only one Unified CM IP address in this page, the other service provider IP addresses in this Unified CM cluster will automatically appear in the list of Available service providers (both AXL and Call Control service providers).

Step 5 The list of Available Call Control Service Providers is also updated automatically for the newly selected service provider. Select and move the required Unified CM servers from the Available Call Control Service Provider list to the Selected Call Control Service Provider list using the right arrow.
If you do not select the required Call Control Service Providers for the new Unified CM server, the MediaSense Call Control Service will be Out Of Service (OOS) and the outbound call recording will be disabled.

Caution If you modify the Unified CM cluster and do not select the required call control service providers for the new Unified CM server, the MediaSense call control service will be out of service (OOS) and outbound call recording will be disabled.

Note If you modify the Unified CM service provider configuration, you must also reconfigure the MediaSense API users. If you do not reconfigure the corresponding users, you will not be able to sign in to use your MediaSense APIs.

Step 6 Click the **Save** icon at the top of the Cisco Unified CM Configuration web page to save your changes.
The MediaSense server validates the Selected Call Control Service Providers and saves this information to the database.

MediaSense setup with Finesse

This section provides the information required to set up MediaSense so that all Finesse supervisors can use the Search and Play application (without additional authentication). This is an optional feature.

Cisco Finesse configuration

Use the Finesse configuration screen to identify two IP addresses by which Finesse and MediaSense can communicate user authentication information between the two systems.

Procedure

Step 1 From MediaSense Administration, select **Administration** > **Cisco Finesse Configuration**.

Step 2 In the **Primary Cisco Finesse IP or hostname** field, enter the IP address or hostname of the Finesse server that you want as the primary server for MediaSense to communicate with.

Step 3 Optionally, in the **Secondary Cisco Finesse IP or hostname** field, enter the IP address or hostname of the Finesse server that you want as the secondary server for MediaSense to communicate with.
Note that in order to define a secondary server, a primary server must first be defined.

Step 4 Click the **Save** icon at the top of the page to save your changes.
To reset the servers, click **Reset** and repeat these steps.

Provision users for MediaSense deployment

You can provision Unified CM end users as Application Programming Interface (API) users in MediaSense deployments. Only the MediaSense application administrator can provide API access for Unified CM end users.

MediaSense API users

The MediaSense open Application Programming Interface (API) list is available for third-party users to securely perform the following functions:

- Pause and resume, hold and resume, or conference and transfer a recording while in progress.
- Control a recorded session.
- Search and manage existing recordings.
- Monitor a live session.

MediaSense APIs provide an alternate to the functionality that is available through the MediaSense web interface. Using these APIs, users can create customized client applications. System integrators and developers who want to use MediaSense to integrate with other Unified Communications software or any third-party software applications need to have access to the MediaSense API. See Unified CM user information and MediaSense setup, on page 47.

API user configuration

MediaSense API users can use various MediaSense APIs to perform various functions with the captured recordings.

For more details about API usage, you must first provision Unified CM end users as API users in MediaSense Administration.

Caution If you modify the Unified CM cluster configuration, you must reconfigure the MediaSense API users. If you do not reconfigure the corresponding users, you will not be able to sign in to use your MediaSense APIs.

Procedure

Step 1 From MediaSense Administration, select **Administration** > **MediaSense API User Configuration** .
The **MediaSense API User Configuration** screen displays the **MediaSense User List** of the first 75 configured MediaSense API users. You can sort the list by any of the columns, in both ascending and descending order.

Step 2 To modify the list, click **Manage MediaSense Users**.
The **MediaSense API User Configuration** screen displays the available Unified CM users in the **Available Unified CM Users** list and the configured API users in the **MediaSense API Users** list.

Step 3 To search for users from the **Unified CM** list, enter the appropriate user ID (or part of the ID) in the **Search for Available Unified CM Users** field and click **Search**.
The search results display all available users where the ID of the user contains the specified search text. The results of the search are listed in random order. If the search finds more than 75 users, only the first 75 are listed.

Note The returned list only displays users that are available (not already provisioned for MediaSense). As a result, the list may contain fewer than 75 users even if there are that many end users in Unified CM that meet the search criteria.

Step 4 Use the left and right arrows to make the required modifications to the MediaSense user list and click **Save**.
The **MediaSense API User Configuration** screen refreshes to display your saved changes.

Click **Reset**, to have all settings revert to the previously configured list of users.

Click **Back to User List** to return to the MediaSense User List .

Storage management agent

MediaSense deployments have a central storage management service called the storage management agent (SM agent). The SM agent provisions media, monitors storage capacity, and alerts system administrators when various media and storage-related thresholds are reached.

Pruning Options

MediaSense deployments provide pruning options to address varied deployment scenarios. Pruning options are specified on the **Administration** > **Prune Policy Configuration** page.

These pruning options allow you to enter the following modes:

- New Recording Priority mode—In this mode, the priority is on providing space for newer recordings, by automatically pruning older recordings. This is the default behavior. The default age after which recordings will be pruned is 60 days. Old recordings will also be pruned if disk space is required for new recordings.
- Old Recording Retention mode—In this mode, priority is placed on retaining older recordings. Old recordings are not automatically pruned.

To focus priority on making new recordings in the New Recording Priority mode, mark the check box for *Automatically prune recordings after they are more than __days old, and when disk space is needed for new recordings*. When this check box is marked, a recording is deleted when one of the following conditions is met:

- The age of the recording is equal to or greater than the retention age that you specify in the field for this option (valid range is from 1 to 3650 days).

  For example, if you are within your disk usage percentage and if you automatically wish to delete all recordings older than 90 days, you must enter 90 in the *Automatically prune recordings after they are more than __days old, and when disk space is needed for new recordings* field. In this case, all recordings which are older than 90 days are automatically deleted. The default value is 60 days.

  Note A day is identified as 24 hours from the precise time you change this setting—it is not identified as a calendar day. For example, if you change the retention period at 23.15.01 on April 2, 2010, the specified recordings will be deleted only at 23.15.01 on April 3, 2010. The recordings will not be deleted at 00:00:01 on April 3, 2010.

- The disk usage has crossed the 90% mark. When the disk usage crosses the 90% mark, some sessions are pruned based on age criteria. This pruning continues until the disk usage is acceptable.

  Note
  - When you use this option to automatically delete recordings, MediaSense removes older recording data irrespective of contents. The priority is provided to newly recorded media and disk space is overwritten to accommodate new recordings.
  - If you wish to use the preceding option (New Recording Priority mode) and, at the same time, wish to protect a particular session from being automatically pruned, be sure to store that session in MP4 format, download the MP4 file, and save it to a suitable location in your network. You can also use the `downloadUrl` parameter in the Session Query APIs and download the raw recording to a location of your choice.

When sessions are pruned, the corresponding metadata is not removed from the database; nor is the data marked as deleted in the database. MediaSense also provides options (radio buttons) that allow you to choose (or decline) to have this associated session data removed automatically.

The following options allow you choose how to handle data associated with pruned sessions:

- To have MediaSense remove the associated data automatically, select the *Automatically remove associated data and mp4 files* radio button.
- If you select the *Do not automatically remove associated data and mp4 files* radio button, the associated data will not be removed automatically. Instead, your client application must explicitly remove automatically pruned recordings, by way of the `getAllPrunedSessions` API and the `deleteSessions` API. When the `deleteSessions` API is executed, the metadata is *marked* as deleted, and the mp4 files are deleted.

To place the priority on retaining older recordings (Old Recording Retention mode), uncheck the *Automatically prune recordings after they are more than __days old, and when disk space is needed for new recordings* check box. If this check box is unchecked, Cisco MediaSense does not automatically prune data. Instead, you must use your client application to remove unwanted data and free up disk space. See the *Developer Guide for Cisco MediaSense*) at http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html for more information.

Caution If you do not clean up unwanted data periodically, the call control service rejects new calls and drops existing recordings at the emergency threshold level (ENTER_EMERGENCY_STORAGE_SPACE). See Storage threshold values and pruning avoidance, on page 54 for more details.

Prune Policy Configuration

Use the following information to set up automatic pruning (New Recording Priority mode).

To specify that MediaSense should automatically prune recordings based on age and disk space (New Recording Priority mode) use the *Automatically prune recordings after they are more than __days old, and when disk space is needed for new recordings* check box. Be sure to specify the age for recordings (the age at which they will be pruned) in the field provided.

Warning When you change the number of days to delete old recordings, or change the pruning policy (check or uncheck the check box) your service will be disrupted and you must restart MediaSense Media Service for all nodes in the cluster. Be sure to make this change during your regularly scheduled downtime to avoid service interruptions.

Warning If MediaSense is not configured to automatically prune recordings, and you change this behavior by using the *Automatically prune recordings after they are more than__days old, and when disk space is needed for new recordings* option, a significant amount of pruning activity may begin. This increase in pruning activity could temporarily impact system performance.

To configure the age threshold (number of days) for automatic deletion of old recordings, follow this procedure:

Procedure

Step 1 From MediaSense Administration, select **Administration** > **Prune Policy Configuration** .
The MediaSense Prune Policy Configuration web page opens to display the configured number of days in the *Automatically prune recordings after they are more than __days old, and when disk space is needed for new recordings* field. The valid range is from 1 to 3650 days, the default is 60 days.

Step 2 Change the value in this field as you require, and ensure that the corresponding check box is checked.

Step 3 If you want MediaSense to automatically remove associated session data and mp4 files, select the *Automatically remove associated data and mp4 files* radio button. If you want your client application to handle removal of associated data and mp4 files, select the *Do not automatically remove associated data and mp4 files radio button*. After you specify your options, click **Save** to apply the changes.
The page refreshes to display the new settings.

Storage threshold values and pruning avoidance

An API event is issued each time the media disk space (which stores the recorded media) reaches various thresholds. You can uncheck the *Automatically prune recordings after they are more than __days old, and when disk space is needed for new recordings* option and judiciously follow all threshold alerts by deleting unwanted recordings. By doing so, you can conserve space for the recordings that are required.

The other option to avoid data loss is to check the *Automatically prune recordings after they are more than __days old, and when disk space is needed for new recordings* option and then save the required recordings as MP4 files to a safe location in your network.

For more information about these options see Pruning Options, on page 52.

The threshold value percentages and the corresponding implications are provided in the following table:

Table 3: Storage threshold values

Threshold storage	Percentage	Description
ENTER_LOW_ STORAGE_SPACE	Recorded media crossed the 75% storage utilization mark.	First warning to indicate that the disk storage is running into low space condition.
EXIT_LOW_ STORAGE_SPACE	Recorded media usage dropped below 70% utilization mark.	The disk storage is exiting the low storage space condition.

Threshold storage	Percentage	Description
ENTER_CRITICAL_ STORAGE_SPACE	Recorded media crossed the 90% local storage utilization mark.	Second warning. When entering this condition, action must be taken to guarantee future recording resources on this server. If operating in the old recording retention mode (no automatic pruning), new recording sessions are not accepted when you reach this threshold. If operating in the new recording priority mode, older recordings are subject to automatic deletion (to make room for new recordings).
EXIT_CRITICAL_ STORAGE_SPACE	Recorded media usage dropped below the 85% utilization mark.	The disk storage is exiting the critical storage space condition. At this point the local server is still considered to be low on resources. In the new recording priority mode, the default pruning stops and only retention-based pruning is in effect.
ENTER_EMERGENCY_ STORAGE_SPACE	Recorded media crossed the 99% storage utilization mark.	Last warning. When the disk storage enters this condition, you must take action to guarantee future recording resources on this server. In addition to actions taken when in CRITICAL condition, all ongoing recordings are dropped and the node is considered out-of-service for recording purposes.
EXIT_EMERGENCY_ STORAGE_SPACE -	Recorded media usage dropped below the 97% utilization mark.	The disk storage is exiting the emergency storage space condition. At this point, the local server is still considered to be low on resources and new recording sessions are still not accepted in the retention priority mode. In new recording priority mode, the server will process new recording requests.

See the *MediaSense Developer Guide* at http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html for more details about the corresponding APIs, Events, and error code descriptions.

The following APIs and events correspond to this task:

- Event Subscription APIs
  - subscribeRecordingEvent
  - unsubscribeRecordingEvent
  - verifyRecordingSubscription
- The storageThresholdEvent Recording Event

System thresholds

The storage thresholds are monitored by the storage management agent (SM agent) on a per server basis. The thresholds are for the total space used on each server and do not attempt to distinguish between the media types being stored.

Periodic storage capacity checks are performed to maintain the health of the system and recordings.

View disk space use

To monitor the disk space used on each server in the MediaSense cluster, follow the procedure identified in this section.

Caution If the server is not started, or is in an unknown state or is not responding, then the disk use information is not displayed. You may need to verify the state of your server to verify if it is reachable (using the `ping` command).

See Storage threshold values and pruning avoidance, on page 54 for more information about threshold value percentages.

Procedure

Step 1 From MediaSense Administration, select **System** > **Disk Usage**.
The MediaSense Server Disk Space Usage web page is displayed.

Step 2 In the Server Disk Space Usage web page, select the required server from the Select Server drop-down list and click **Go**.
The Server Disk Space Usage web page refreshes to display the disk space used for the selected server in gigabytes (GB) or terabytes (TB) depending on the size of the disk drive. This page is read-only.

If the selected server does not display any information in this web page, you may receive an alert informing you that the disk usage information is not available for this server. If you receive this message, verify the state of the server to ensure that the server is set up and functioning.

Storage use information obtained using HTTP

You can also obtain the current storage use information using HTTP GET requests. The URL for accessing this information is:

```
http://<server-ip-address>/storagemanageragent/usage.xml
```

The storage use information is provided in an XML format.

- Example 1— Does not use any media disks:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <storageUsageInfo date="Oct 26 2010" time="13:24:22"
gmt="1288124662599">
- <partitions>
  <partition name="/common" size="655G" usage="29%" />
  </partitions>
  </storageUsageInfo>
```

- Example 2—Uses two media partitions:

```
  <?xml version="1.0" encoding="UTF-8" ?>
<storageUsageInfo date="Oct 26 2010" time="13:10:53" gmt="1288123853753">

   <partitions>
    <partition name="/media1" size="200G" usage="5%" />
    <partition name="/media2" size="200G" usage="50%" />
    </partitions>
    </storageUsageInfo>
```

Note The number of media partitions directly corresponds to the number of configured media disks. If you configure two media disks, you see two media partitions: /media1 and /media2.

Storage use information obtained by using Unified RTMT

The disk use monitoring category charts the percentage of disk use for the common and media partitions. It also displays the percentage of disk use for each partition (Active, Boot, Common, Inactive, Swap, Shared Memory, Spare) in each host. The Log Partition Monitoring Tool is installed automatically with the system and starts automatically after the system installation process is complete.

Note If more than one logical disk drive is available in your system, the Cisco Unified Real Time Monitoring Tool (Unified RTMT) can monitor the disk use for the additional partition in the Disk Usage window.

Unified RTMT displays all partitions in MediaSense and in the Unified Communications OS. Depending on the number of disks installed, the corresponding number of media partitions are visible in the Disk Usage window. If you do not install any media partitions, only Partition Usage (common media) is visible.

Caution The MediaSense SM agent must be running to view media disk use information in both the Disk Usage window and the Performance window in Unified RTMT.

While real time media partition use is visible in the Disk Usage window, historical partition use details are visible as performance counters in the Performance window.

Incoming Call Configuration

MediaSense enables you to assign one incoming call rule to each endpoint in the contact center. Acting on an incoming call rule, each endpoint can:

- Record incoming calls
- Play an outgoing media file once
- Play an outgoing media file continuously
- Reject incoming calls

MediaSense provides an editable system default rule. Until you assign another action as the system default rule, MediaSense defaults to recording the call. This system default rule appears in the first row in the list of incoming call rules on the **Incoming Call Configuration** screen, regardless of how you sort the list.

If no incoming call rule has been assigned to an endpoint, MediaSense falls back on the system default rule when an incoming call arrives at that endpoint.

Incoming Call Rules List

The **Incoming Call Configuration** screen displays a read-only list of the incoming call rules for each endpoint in the contact center. Displayed in rows, you can view the address of an endpoint and the action which is incoming call rule for that endpoint. When the call rule is **Play Once** or **Play Continuously**, the list also displays the title of the media file that is assigned to that endpoint.

System-assigned lock icons identify any incoming call rules which cannot be edited or deleted.

Address Requirements

Valid addresses must:

- Consist of the legal user portion of a SIP URL. For example, the legal user portion of the SIP URL john123@yourcompany.com is the user name, john123.
- Be assigned to only one incoming call rule at a time. You can assign this rule or do nothing and allow the endpoint to use the editable system default rule.

Add Incoming Call Rule

An endpoint address can be assigned to only one incoming call rule. If you do not assign an incoming call rule to an endpoint, the endpoint uses the system default call rule.

Procedure

Step 1 From the **Administration** menu, select **Incoming Call Rule Configuration**.

Step 2 On the **Incoming Call Rule Configuration** toolbar, click **Add**.

Step 3 On the **Add Incoming Call Rule** screen, go to the **Address** field and enter the legal user portion of a SIP URL.

Example:
For example, if the SIP URL is 578452@yourcompany.com, its legal user portion is john123. Often the legal user portion of SIP URLs for Videos in Queue are all numeric. So for a SIP URL such as 5551212@yourcompany.com, the legal user portion is simply 5551212.

Step 4 From the **Action** drop-down list, select an incoming call rule. Possible values include Play Continuously, Play Once, Record, or Reject.

Step 5 Click **Save**.
MediaSense returns you to the **Incoming Call Rule Configuration** screen. The top of this screen displays the message **Rule saved**. The new incoming call rule appears in the **Incoming Call Rules** list.

Edit Incoming Call Rule

You can edit an incoming call rule by changing its address, changing its action, or changing both its address and its action. The address must be the legal user portion of a SIP URL.

Procedure

Step 1 From the **Administration** menu, select **Incoming Call Rule Configuration**.

Step 2 At the bottom of the **Incoming Call Rule Configuration** screen, go to the **Incoming Call Rules** list and select the radio button for the call rule that you want to edit.

Step 3 On the **Incoming Call Rule Configuration** toolbar, click **Edit**.

Step 4 (Optional) On the **Edit Incoming Call Rule** screen, go to the **Address** field and enter the legal user portion of a different SIP URL.

Example:
If the SIP URL is 5551212@yourcompany.com, the legal user portion is 5551212.

Step 5 (Optional) On the **Edit Incoming Call Rule** screen, go to the **Action** drop-down list and select a different incoming call rule for the endpoint.

Step 6 If you selected **Play Once** or **Play Continuously** as the Action, go to the **Media File** drop-down list and select a media file.

Step 7 Click **Save**.
MediaSense returns you to the **Incoming Call Rule Configuration** screen. The top of this screen displays the message **Ruled saved**. The edited incoming call rule appears in the **Incoming Call Rules** list.

Edit System Default Incoming Call Rule

The System Default incoming call rule always appears in the first row of the **Incoming Call Rules** list on the **Incoming Call Configuration** screen. The System Default call rule applies to any endpoint to which you have not assigned another incoming call rule.

When MediaSense is installed, it defines the System Default incoming call rule as **Record**. You can change this call rule to **Play Once**, **Play Continuously**, or **Reject**. If you want to change it again later, you can change it back to **Record** or to another incoming call rule.

If you choose not to edit System Default call rule, it remains as **Record**.

Procedure

Step 1 From the **Administration** menu, select **Incoming Call Rule Configuration**.

Step 2 At the bottom of the **Incoming Call Rule Configuration** screen, go to the **Incoming Call Rules** list and select the radio button for the System Default call rule.

Step 3 On the **Incoming Call Rule Configuration** toolbar, click **Edit**.

Step 4 On the **Edit Incoming Call Rule** screen, go to the **Action** drop-down list and select a different incoming call rule.

Step 5 If you selected **Play Once** or **Play Continuously**, go to the **Media File** drop-down list and select a file.

Step 6 Click **Save**.
MediaSense returns you to the **Incoming Call Rule Configuration** screen. The top of this screen displays the message **Ruled saved**. The edited System Default call rule appears at the top of the **Incoming Call Rules** list. Any changes that you made in **Action** or in the selection of media file appear in the respective columns of the first row.

Delete Incoming Call Rule

Most incoming call rules can be deleted one at a time. You cannot delete the System Default call rule or any incoming call rule that it marked with a system-assigned lock icon.

Procedure

Step 1 From the **Administration** menu, select **Incoming Call Rule Configuration**.

Step 2 From the **Incoming Call Rules** list, select the radio button for the Incoming Call Rule that you want to delete.

Step 3 Click **Delete**.

Step 4 In the confirmation dialog box, click **OK**.
The top of the **Incoming Call Rule Configuration** screen displays the message **Rule deleted**. The **Incoming Call Rule List** no longer displays the deleted rule.

Media File Management

You can configure MediaSense to play an outgoing message when a caller is waiting for an agent to answer the incoming call. You can also configure MediaSense to play an outgoing message when an agent places a caller on hold. In either scenario, the message can be configured to play continuously or to play only once.

You can configure MediaSense to simply play a system default message for all calls (whether waiting or on hold) or you can configure it to play a different message for different purposes.

For example, if a caller dials the sales department number, then you might want an advertising video to play while they are waiting for an agent. Otherwise, if a caller dials the number for the CEO, then you might want an animated formal corporate logo to play. You would upload two media files in this example, and associate one file to the SIP address for sales department's outgoing message and the other file to the SIP address for the CEO's outgoing message (with both of these SIP addresses configured in MediaSense).

You can upload one media file at a time on the primary node in a MediaSense cluster. The primary node accepts the file and then sends copies of it to the secondary node and to any expansion nodes in the cluster. Each node then converts the file to a format that MediaSense can play as an outgoing message. MediaSense shows these converted files in the **Media File List** on the **Media File Management** screen and in the top table on the **Media Files Detail** screen.

Media File States

Each uploaded media file can be in one of several states. These states are shown in the **Media File List** on the **Media File Management** screen and in the tables on the **Media File Details** screen.

Possible media file states include:

- **Processing**: When your uploaded media file is in the processing state, the primary node distributes the file to all nodes in the cluster. Each node processes the file and when processing finishes, the uploaded file enters the Ready state. When you begin the process of adding a new node to the cluster, all existing uploaded media files go into processing state and remain there until the new node has completed its processing steps for those media files. (Note that the files can still be played normally as long as any node has them in ready state.)
- **Ready**: The uploaded file has finished processing on all nodes. It is ready to be played as an outgoing message from one or more assigned SIP addresses.
- **Deleting**: Deleting a file may take some time. After a file has been deleted from all nodes, it disappears from the MediaSense user interface and cannot be recovered. If you want to upload the same media file again, you can. You must, however, go through the entire processing phase again.
- **Error**: Files that have not been successfully processed are shown in the error state. Files in this state can be deleted or redeployed to resolve the error condition.

Play Media Files

Users can play or download media files in the ready state directly from the **Media File Management** summary or detail pages. Click on the green arrow at the right side of the screen to play the media file -- if an appropriate program for playing mp4 files is installed on your computer. (Depending on your browser and configuration, you may be prompted to select a program to play the file, or the file may just not play).

Also depending on your browser, you can right click the green arrow and select an option to download the file to a location of your choice.

Media File Details

The **MediaSense File Details** screen displays information about individual media files in two tables. The top table displays details at the cluster level. The bottom table displays details at the node level.

The state values in both tables appear to be the same. Possible states in both tables include Processing, Ready, Deleting, and Error. However, these state values mean different things in each table. In the top table, states are reported are aggregate values that reflect all nodes in the cluster. For example, as long as at least one node

is processing a media file, the cluster state value is reported as Processing. The cluster state does not change to Ready until the media file is ready on all nodes in the cluster.

In the bottom table, state values are reported at the node level. The states, Processing, Ready, Deleting, and Error, are shown for the uploaded media file as it is on each separate node in the cluster. Media files can reflect different states on different nodes at the same time. For example, a media file might be shown as Processing on the secondary node and shown as Ready on an expansion node at the same time.

Add Media File

Media files can only be added one at a time. All other media files in the system must be in a ready state when you upload a media file. If you attempt to upload a file when another media file is uploading, processing, or in an error state; you risk causing additional errors.

Note A user may encounter an error if they begin to upload a file at the same time as another user on the system. If an unexpected error is returned to the browser, refresh the Media File Management page and wait for the other upload to complete, then restart the upload.

Files to be added must be in MP4 format and meet the following specifications:

- Must contain one video track and one audio track.
- Video must be H.264 encoded.
- Audio must be AAC-LC encoded.
- Audio must be monaural.
- The entire MP4 file size must not exceed 2GB.

Procedure

Step 1 From the **Cisco MediaSense Administration** menu, select **Media File Management**.

Step 2 On the **Media File Management** toolbar, click **Add**.

Step 3 On the **Add Media File** screen, enter a unique title for the media file.

Step 4 (Optional) Enter a description of the file.

Step 5 Browse and select a media file in the **File** field.

Step 6 Click **Save**.
Note: With some browsers, MediaSense can detect the size of the file that is being uploaded and will show an immediate error if it knows there isn't enough space available on disk to handle it. If MediaSense cannot detect the file size immediately, the upload process will start and then fail (putting the file in the error state) if it does not have enough space.

MediaSense uploads the file and returns you to the **Media File Management** screen. The uploaded file appears in the **Media File List**.

Edit Media File

You can edit the title and description of a media file that you have uploaded to MediaSense.

Procedure

Step 1 From the **Administration** menu, select **Media File Management**.

Step 2 Go to the **Media File List** at the bottom of the **Media File Management** screen. Select the radio button for the media file with the title or description that you want to edit.

Step 3 Click **Edit**.

Step 4 (Optional) In the **Edit Media File** screen, edit the title.

Step 5 (Optional) In the **Edit Media File** screen, edit the description.

Step 6 Click **Save**.
The top of the **Media File Management** screen displays the message **File Saved**. If you edited the media file title, the edited title appears in the **Media File List**. If you did not edit the title, and only edited the description, there is no change in media title in the **Media File List**. You know the change was made because of the **File Saved** message.

Redeploy Media File

You can redeploy a media file that has already been uploaded to MediaSense if it is displaying an error status.

Procedure

Step 1 From the **Administration** menu, select **Media File Management**.

Step 2 Identify the file showing an error status (red x icon).

Step 3 Select the radio button for the file with the error condition.

Step 4 Click **Redeploy**.
Note that the file status now changes from Error to Processing.

Step 5 Alternately, you can click on the file name to open the detail page and click the Redeploy button on the detail page.

Delete Media File

Media files can be deleted one at a time. After a media file has been deleted, it cannot be recovered. All other media files in the system must be in a Ready state when you delete the file.

Procedure

Step 1 From the **Administration** menu, select **Media File Management**.

Step 2 Go to the **Media File List** and verify that all other media files in the list are in a Ready state.

Step 3 From the **Media File List**, select the radio button for the media file that you want to delete.

Step 4 Click **Delete**.
MediaSense permanently deletes the file. The state value is shown as Deleting (and the Redeploy button for that file is disabled). After the file is deleted, it disappears from the MediaSense user interface.

Refresh media file

Use the Refresh button on the Media File Management summary page or the Media File Detail page to view updated information for a file when uploading a new video. When a file is uploaded through the Add Media File page, the user is returned to the Media File Management page. The file may be in the processing stage for a while, but there is no automatic update of when processing is complete.

Procedure

Step 1 From the **Administration** menu, select **Media File Management**.

Step 2 Click **Refresh** to update the status of all files.

Step 3 Alternately, select an individual media file and open the Media File Detail page for that file, then click **Refresh**.

MediaSense server configuration

Procedure

Step 1 From the **Cisco MediaSense Administration** menu, select **System** > **MediaSense Server Configuration**.

Step 2 In the **MediaSense Server Configuration** screen, click **Add MediaSense Server**.
The **Add MediaSense Server** screen in the primary node opens.

Step 3 If your installation uses DNS, enter the hostname of the server that you want to add. If your installation does not use DNS, enter the IP address of the server that you want to add.

Step 4 (Optional) Enter the description of the server that you want to add.

Step 5 (Optional) Enter the MAC address of the server that you want to add.

Step 6 Click **Save**.

Step 7 MediaSense displays a confirmation message near the top of the screen.
You see the configuration details of the server that you added in the **MediaSense Server List**. Note that the server type is "UNKNOWN" at this stage of the installation.

Media partition management

Use the **Media Partition Management** page to manage the media partitions used on the MediaSense node that you are currently logged into. The page shows the amount of disk space formatted for each media partition and the percentage of disk space used. Access the **Configure Media Partitions** page to increase the size of the media partitions.

Fresh installations of MediaSense have media partitions labeled as /recordedMedia and /uploadedMedia. To increase the size of the media partitions after initial installation, you must add additional disks drives to the host (using VMware). Once the system recognizes the new disks, you can increase the size of both of these partitions until they reach a maximum of 15 TB each. Any increase in size is permanent (the size cannot be reduced after having been increased).

- The /recordedMedia partition stores up to 15 TB of recordings of live and completed incoming calls.
- The /uploadedMedia partition stores up to 15 TB of outgoing media clips which MediaSense plays when a caller is on hold or a caller is waiting in a queue.

Upgraded installations of MediaSense have no media partition that is labeled /recordedMedia. Instead, they have from one to six numbered media partitions, such as media1. Each numbered media partition is fixed in size and stores from 200 GB to 2 TB of recordings of incoming calls. Recordings can be stored in these numbered partitions only until these fixed-size partitions become full. You cannot reconfigure these numbered media partitions to increase their size. Depending on the number of media partitions, each upgraded installation can store from 200 GB to 12 TB of recordings of incoming calls.

Upgraded installations have one media partition that is labeled /uploadedMedia. As in fresh installations, this partition stores up to 15 TB of outgoing media clips that MediaSense plays when a caller is on hold or a caller is waiting in a queue. Similar to fresh installations, you can increase the size of the /uploadedMedia partition on uploaded installation to 15 TB and any increase in size is permanent.

Note When increasing the size of the /uploadedMedia partition, ensure that you increase the size of the media partition on **all** nodes in the MediaSense system.

Configure Media Partitions

Use this procedure to increase the physical size of the media partitions on the MediaSense node on which you are currently logged in.

- On fresh installations, you can configure the /recordedMedia partition and the /uploadedMedia partition.
- On upgraded installations, you can configure the /uploadedMedia partition. You cannot configure the numbered media partitions on upgraded installations.

Note Configure media partitions only during a maintenance period. The Media Service records no calls while you configure media partitions. It records calls again after you finish.

Procedure

Step 1 Confirm that the maintenance period has begun and that no incoming calls are being recorded.

Step 2 Using VMware VSphere, add one or more virtual disks to the MediaSense virtual machine.

Step 3 From the **Cisco MediaSense Administration** menu, select **System** > **Manage Media Partitions**.

Step 4 On the **Manage Media Partitions** page, click **Configure Media Partitions**.
Your newly added disks should appear in the list as "Unassigned". If they do not, wait a few minutes and refresh the page until they do.

Step 5 On the **Configure Media Partitions** page, go to the **Available Disk List** table. Open the **Media Partition** drop-down list for the disk that you want to assign. Select the media partition to which you want to assign the disk.

Step 6 Repeat the previous step as needed.

Step 7 Click **Save**.
An alert message tells you that the disk assignment cannot be reversed. You cannot reduce the media partition size after you increase it.

Step 8 In the alert message box, click **OK**.

Step 9 Wait while MediaSense configures the media partitions. Do not click buttons or close the window.
MediaSense displays a confirmation message. The **New Unformatted Size** column in the **Media Partitions List** table displays the increased size of the media partition or partitions to which you added a disk or disks. The Media Service starts recording incoming calls again.

Step 10 Click **Back to Media Partition Management**.
The **Media Partition Management** page re-opens. Changed values appear in the **Total Formatted Partition Size** column of the **Media Partitions List** table.

Event management

The MediaSense API service issues notifications about events taking place in a MediaSense cluster. For example, events may be created when the storage disk space reaches various thresholds, when a new recording session is started, when an existing recording session is updated or ended, or when a tag is added or deleted from a session.

Enable event forwarding

The Event Subscription APIs allow applications to subscribe, verify the subscription, and unsubscribe for all event notifications. For more information, see the *MediaSende Developer Guide* at http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html. If a MediaSense deployment has two servers (primary and secondary), the third-party client applications must subscribe to each server separately to receive events generated on each server.

MediaSense Administration provides a cluster-wide property to enable or disable event forwarding between the primary and secondary servers in any MediaSense cluster. By default, forwarding is disabled and you need to explicitly enable this feature to receive notification of all events. If you enable this feature, you receive events generated on both servers—you do not need to subscribe explicitly to each of the two servers.

Note The third-party client must subscribe to either the primary or the secondary server to start receiving event notifications for either or both servers. If you enable event forwarding, then the third-party client can subscribe to only one server (either primary or secondary) to get all events.

To enable event forwarding between the primary and secondary servers in the MediaSense cluster, follow this procedure.

Procedure

Step 1 From MediaSense Administration, select **System** > **Event Management**.
The MediaSense Event Management web page appears.

Step 2 In the Event Management web page, check the **Enabled Event Forwarding** check box to enable event forwarding between the primary and secondary server in this cluster. Click **Save**.
The third-party client starts receiving notifications for all events on both servers (regardless of the server in which you enable this feature).

MediaSense setup with Cisco Unified Border Element

With the Cisco Unified Border Element (CUBE) deployment model, MediaSense requires Unified CM authentication for all MediaSense users. All Unified CM User ID restrictions apply.

Manage Unified CM users

The Administrative XML Layer (AXL) authentication allows you to enter the Unified CM cluster and retrieve the list of Unified CM servers within a cluster. During the AXL authentication, if the Unified CM Publisher is offline or not available, you can provide the next available Unified CM Subscriber for the AXL authentication. The AXL Administrator username may not be same as the Unified CM Administrator username for that cluster. Be sure to add the username for the AXL Administrator to the Standard Unified CM Administrators group and “Standard AXL API Access” roles in Unified CM.
Do the following tasks before you start using MediaSense servers for a CUBE deployment:

- Configure and deploy the required Unified CM cluster and users to before you configure MediaSense. See the Unified CM documentation at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
- Review the Supported Deployments section for information about Unified CM authentication.
- Ensure that you have the Unified CM IP address, AXL Admin username, and AXL Admin Password that you need to complete the MediaSense post-installation tasks.

Cisco MediaSense provisioning for CUBE

After you have created the AXL users in Unified CM, you must assign the Unified CM user (or users) using the MediaSense UI by selecting and assigning the Unified CM AXL user as a MediaSense API user.

Caution To enhance interoperability with third-party SIP devices, CUBE dial-peers (by default) enable Early-Offer for outgoing voice and video calls. *Do not change this Early-Offer default for MediaSense deployments*.

Complete the following tasks to ensure that MediaSense is provisioned for a CUBE deployment:

- Select AXL service providers, on page 47
- Replace Unified CM service providers, on page 49
- Provision users for MediaSense deployment , on page 50

Note You do not need to configure call control service providers in MediaSense for any CUBE deployment.

CUBE and MediaSense setup

The CUBE application uses the CLI to access and configure CUBE to enable media recording in MediaSense.

Complete the tasks identified in this section to access and configure CUBE for MediaSense:

- CUBE gateway accessibility, on page 68
- CUBE view configuration commands, on page 68
- Global-level interoperability and MediaSense setup, on page 69
- Dial-peer level setup, on page 71

CUBE gateway accessibility

To access CUBE, use SSH or Telnet to enable secure communications. SSH or Telnet sessions require an IP address, a username, and password for authentication. You can obtain these details from your CUBE administrator. See the following table and the CUBE documentation at http://www.cisco.com/go/cube for more information.

Table 4: CUBE access information

Field	Description
IP address	An IP address for the CUBE gateway.
Username	Username configured on the gateway device.
Password	Password configured for this user name.

CUBE view configuration commands

Before you begin any CUBE configuration tasks, be sure to view and verify the existing CUBE configuration.

The following table lists the related IOS-based (CLI) commands to view and verify an existing CUBE configuration.

Table 5: IOS commands to view CUBE configuration

Command	Description
`show running-config`	Displays the existing configuration for this CUBE gateway.
`show startup-config`	Displays the startup configuration for this CUBE gateway.
`show version`	Displays the IOS version being used in this CUBE gateway.
`show call active voice summary`	Displays the number of active SIP calls.

Global-level interoperability and MediaSense setup

To allow interoperability with MediaSense, the CUBE configuration must be added either in dial-peer level or global-configuration level.

Setup global level

Procedure

Step 1 Connect to your CUBE gateway using SSH or Telnet.

Step 2 Enter the global configuration mode.

```
cube# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
cube(config)#
```

Step 3 Enter VoIP voice-service configuration mode.

```
cube(config)# voice service voip
cube(config-voi-serv)#
```

Step 4 Calls may be rejected with a 403 Forbidden response if toll fraud security is not configured correctly. The solution is to add the IP address as a trusted endpoint, or else disable the IP address trusted list authentication altogether using the following configuration entry:

```
cube(config-voi-serv)# no ip address trusted authenticate
```

Step 5 Enable CUBE and CUBE Redundancy.

```
cube(config-voi-serv)#  mode border-element
cube(config-voi-serv)#  allow-connections sip to sip
cube(config-voi-serv)#  sip
cube(config-voi-serv)#  asymetric payload full
cube(config-voi-serv)#  video screening
```

In the example above, the final 3 lines are only required if video calls are to be passed through CUBE.

Step 6 At this point, you will need to save the CUBE configuration and reboot CUBE.

Caution Be sure to reboot CUBE during off-peak hours.

a) Save your CUBE configuration.

```
cube# copy run start
```

b) Reboot CUBE.

```
cube# reload
```

Step 7 After you reboot CUBE, configure the media class to determine which calls should be recorded.

```
cube(config-voi-serv)# media class 3
cube(config-voi-serv)# recorder parameter
cube(config-voi-serv)# media-recording 3000
```

Step 8 Exit the VoIP voice-service configuration mode.

```
cube(config-voi-serv)# exit
```

Step 9 Create one voice codec class to include five codecs (including one for video). These codecs will be used by the inbound and outbound dial-peers to specify the voice class.

```
cube(config)# voice class codec 3
cube(config)# codec preference 1 mp4a-latm
cube(config)# codec preference 2 g711ulaw
cube(config)# codec preference 3 g722-64
cube(config)# codec preference 4 g729br8
cube(config)# video codec h264
```

In the example above, the first codec preference and video codec definition are only required if AAC-LD/LATM media is part of the customer's call flow.

Step 10 To simplify debugging, you must synchronize the local time in CUBE with the local time in MediaSense servers.

For example, if you specify the NTP server as 10.10.10.5, then use the following command in CUBE:

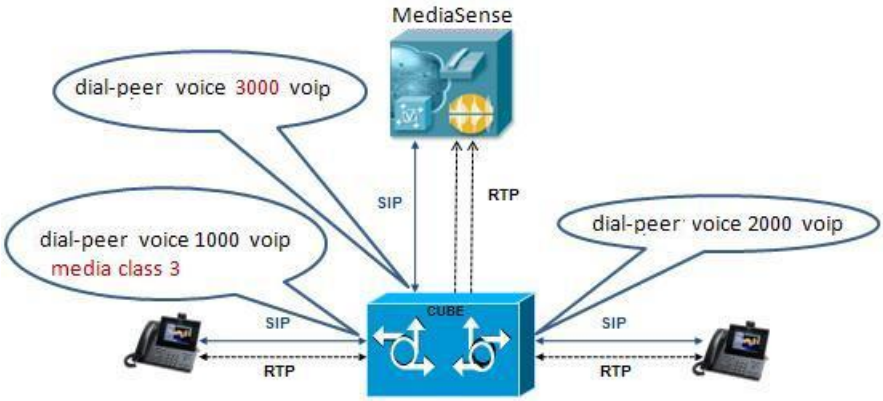
```
cube(config)#  ntp update-calendar
cube(config)#  sntp server 10.10.10.5
```

Dial-peer level setup

Note This information describes a sample configuration. CUBE may be deployed in multiple ways.

Each MediaSense deployment for CUBE contains three dial-peers:

- Inbound dial-peer: In this example, the unique name is 1000
- Outbound dial-peer: In this example, the unique name is 2000
- Forking dial-peer: In this example, the unique name is 3000



Before you begin this procedure, obtain the details for these three dial-peers from your CUBE administrator.

Note The order in witch you configure these three dial-peers is not important.

Set up CUBE dial-peers for MediaSense deployments

This procedure provides an example of how to set up the three dial peers. The specific names and values used are for illustrative purposes only.

Caution This procedure is not a substitute for the actual CUBE documentation. It is a tutorial to provide detailed information about configuring CUBE for MediaSense. See your CUBE documentation at http://www.cisco.com/go/cube for the latest information.

Procedure

Step 1 Configure media forking on an inbound dial peer.

a) Assign a unique name to the inbound dial-peer. In this example, the name is set to '1000'.

```
cube(config)# dial-peer voice 1000 voip
```

The command places you in the dial-peer configuration mode to configure a VoIP dial-peer named '1000'.

b) Specify the session protocol for this inbound dial-peer as 'sipv2' (this value is not optional).

```
cube(config-dial-peer)# session protocol sipv2
```

This command determines if the SIP session protocol on the endpoint is up and available to handle calls. The session protocols and VoIP layers depend on the IP layer to give the best local address and use the address as a source address in signaling or media or both—even if multiple interfaces can support a route to the destination address.

c) Specify the SIP invite URL for the incoming call. In this example, we assume that inbound, recordable calls will have six digits. Here, we assign the first three digits as '123' and the last three digits are arbitrarily chosen by the caller (as part of the destination DN being dialed). This command associates the incoming call with a dial-peer.

```
cube(config-dial-peer)# incoming called-number 123...$
```

d) When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to apply the class to individual dial-peers. In this example, the tag used is '1'.

```
cube(config-dial-peer)# voice-class codec 1
```

This tag uniquely identifies this codec. The range is 1 to 10000.

e) If call is transferred, be sure to propagate the metadata to MediaSense.You can do so by enabling the translation to PAI headers in the outgoing header on this dial-peer.

```
cube(config-dial-peer)# voice-class sip asserted-id pai
```

f) Specify that everything that is going through the inbound dial-peer can be forked. Use the same number that you used to set up global forking (see Set up Global Level). In this example, the number media class is '3'.

```
cube(config-dial-peer)# media-class 3
```

g) Exit the configuration of this inbound dial-peer.

```
cube(config-dial-peer)# exit
cube(config)#
```

Step 2 Configure the outbound dial-peer.

a) Assign a unique name to the outbound dial-peer. In this example, the name is set to '2000'.

```
cube(config)# dial-peer voice 2000 voip
```

The command places you in the dial-peer configuration mode to configure a VoIP dial-peer named '2000'.

b) Specify the session protocol for this outbound dial-peer as 'sipv2' (this value is not optional).

```
cube(config-dial-peer)# session protocol sipv2
```

c) Specify the destination corresponding to the incoming called number. In this example, it is '123...'.

```
cube(config-dial-peer)# destination-pattern 123...$
```

d) When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to apply the class to individual dial-peers. Use the same tag used for the inbound dial-peer. In this example, the tag used is '1'.

```
cube(config-dial-peer)# voice-class codec 1
```

e) Specify the primary destination for this call. In this example, we set the destination to 'ipv4:10.1.1.10:5060'.

```
cube(config-dial-peer)# session target ipv4:10.1.1.10:5060
```

f) Exit the configuration of this outbound dial-peer.

```
cube(config-dial-peer)# exit
cube(config)#
```

Step 3 Configure the forking dial-peer.

a) Assign a unique name to the forking dial-peer. In this example, the name is set to '3000'.

```
cube(config)# dial-peer voice 3000 voip
```

The command places you in the dial-peer configuration mode to configure a VoIP dial-peer named '3000'.

Optionally, provide a description for what this dial-peer does using an arbitrary English phrase.

```
cube(config-dial-peer)# description This is the forking dial-peer
```

b) Specify the session protocol for this forking dial-peer as 'sipv2' (this value is not optional).

```
cube(config-dial-peer)# session protocol sipv2
```

c) Specify an arbitrary destination pattern with no wildcards. Calls recorded from this CUBE will appear to come from this extension. (In the MediaSense Incoming Call Configuration table, this number corresponds to the address field.) In this example, we set it to '3000'.

```
cube(config-dial-peer)# destination-pattern 3000
```

d) When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to apply the class to individual dial-peers. Use the same tag used for the inbound dial-peer. In this example, it is '1'.

```
cube(config-dial-peer)# voice-class codec 1
```

e) Provide the IP address of one of the MediaSense expansion servers (if available) as a destination for the CUBE traffic. In this example, we use a MediaSense server at IP address 10.2.2.20.

Note Avoid using the primary or secondary MediaSense servers for this step as these servers carry the CUBE load and it is best to avoid adding load to the database servers.

```
cube(config-dial-peer)# session target ipv4:10.2.2.20:5060
```

f) Set the session transport type (UDP or TCP) to communicate with MediaSense. The default is UDP. The transport protocol specified with the session transport command, and the protocol specified with the transport command, must be identical.

```
cube(config-dial-peer)# session transport tcp
```

g) Configure a heartbeat mechanism to monitor connectivity between endpoints.
A generic heartbeat mechanism allows Cisco Unified Border Element to monitor the status of MediaSense servers or endpoints and provide the option of timing-out a dial-peer if it encounters a heartbeat failure.

Note If you have configured an alternate dial-peer for the same destination pattern, the call fails over to the next preferred dial-peer. Otherwise, the call is rejected. If you have *not* configured a failover dial-peer, then do not configure options-keepalive.

```
cube(config-dial-peer)# voice-class sip options-keepalive
```

h) Prevent CUBE from sending multipart body in INVITE to MediaSense.

```
cube(config-dial-peer)# signaling forward none
```

i) Exit the configuration of this forking dial-peer.

```
cube(config-dial-peer)# exit
cube(config)#
```

j) Exit the configuration mode.

```
cube(config)# exit
cube#
```

k) Save your CUBE configuration.

```
cube# copy run start
```

CUBE deployments log commands

Cisco Unified Border Element (CUBE) logs errors when calls fail, and it also applies a timestamp to debugging and log messages. The following table identifies some of the useful log commands.

Note Millisecond timestamp provides a better indication of the timing of the various debugs events relative to each other. Do not use msec timestamp to prove performance issues, but to obtain relative information about when events occur.

Table 6: Useful log commands for CUBE deployments

Command	Description
`service timestamp debug datetime msec localtime show-timezone`	Specifies the millisecond (msec) timestamp for various debug events.
`service timestamps log datetime msec localtime show-timezone`	Specifies the millisecond (msec) timestamp for various log events.
`localtime logging buffered 1000000`	Specifies the memory allocation for CUBE logins.
`no logging rate-limit`	Specifies that all log messages should be logged.

Command	Description
`no logging console`	Specifies that log messages should not be displayed on the console.

Access MediaSense Serviceability

After you complete the post-installation setup of MediaSense Administration, you can sign in to MediaSense Serviceability.

Procedure

Step 1 Access MediaSense Serviceability.
You can access MediaSense Serviceability in one of the following ways:

- Enter the following URL in a MediaSense-supported web browser session, where *servername* is the IP address of the server on which you installed MediaSense: **http://***servername***/oraservice**
- From the Navigation drop-down menu in the upper-right corner of the **Administration** window, select **Cisco MediaSense Serviceability** and click **Go**.

Step 2 A security alert message may appear, prompting you to accept the self-signed security certificate. This security certificate is required for a secure connection to the server. Click the required button.
This security message may not appear if you have already installed a security certificate.

The **Authentication** page is displayed.

Step 3 Enter the single sign-in username and password, and click **Log in** .

Note If you have already signed in to MediaSense, you can access MediaSense Serviceability without signing in again.

The welcome page appears after you have successfully logged in. The welcome page displays the version number of the product as well as trademark, copyright, and encryption information.

MediaSense Serviceability

The MediaSense Serviceability menu bar contains the following options:

- **Trace—**Configure log and trace settings for MediaSense components. Once enabled, you can collect and view trace information using the Unified Real-Time Monitoring Tool (Unified RTMT).
- **Tools—**Contains options that allow you to access system tools such as Unified RTMT Plug-ins, manage network services, and control feature services.
- **Help—**Provides access to online help for MediaSense.

After you are in the required administration interface, select one of the following options:

- To display documentation for a single window, click **Help** > **This Page**.
- To verify the version of the administration running on the server, click **Help** > **About** or click the **About** link in the upper-right corner of the window.
- To view the latest version of all documents for this release, click **Help** > **Cisco.com**.

  If you are connected to the external network, this link connects you to the home page for MediaSense (http://www.cisco.com/en/US/products/ps11389/tsd_products_support_series_home.html).
- To view the latest version of the troubleshooting tips for this release, click **Help** > **Troubleshooting Tips** .

  If you are connected to the external network, this link connects you to the Troubleshooting page for MediaSense (http://docwiki.cisco.com/wiki/Troubleshooting_Cisco_MediaSense).

Trace setup

This section provides information about using traces in MediaSense Serviceability Administration.

Trace files

A trace file is a log file that records activity from the MediaSense components. Trace files allow you obtain specific, detailed information about the system so you can troubleshoot problems. The MediaSense system can generate trace information for different services. The generated information is stored in a trace file. To help you control the size of a trace file, you can specify the services for which you want to collect information and the level of information that you want to collect.

Trace information is primarily used by developers to debug problems. Each MediaSense service can consist of several components. Each component can consist of multiple trace flags. You can enable or disable tracing for each component or for the required flags. Unlike logs, trace files are written only at one level. This section describes the trace configuration requirement for MediaSense Serviceability Administration.

Caution If MediaSense Administration is unable to contact the MediaSense configuration service, it uses default trace settings. If the MediaSense configuration service is disabled or stopped, the trace configuration information is not displayed in the corresponding user interface pages. Similarly, if trace configuration is not available for any service, the user interface pages will not display any information for that service.

Differences between tracing and logging:

- Tracing: trace flags are free from detailed, developer-oriented information that is not printed to the logs by default, but only when increased logging is enabled to debug problems.
- Logging: log messages are predefined, higher-level messages that are always printed to the logs and indicate everything for normal system behavior to severe error conditions.

Trace log levels

Trace flag information is stored in the configuration database.

Log Levels identify the MediaSense message level (info and debug) to be generated for each service. The currently-enabled log levels for each service component are identified by a radio button (Log Level column)

in the **Trace Configuration** screen. The currently-enabled trace flags are identified by a check mark (Enabled column) in the **Trace Configuration** screen.

Note There is no log level or trace mask for the Perfmon agent network service.

Caution Because the media service does not support dynamic trace-level change, you cannot create or view a trace file for this service. Trace flags for the media service are used only by TAC and are not available to end users.

MediaSense log information is provided in the following output files:

- ORASERVICE-oraservice.<yyyy-MM-dd>T<HH-mm-ss.SSS>.startup.log: contains debug and info messages (see the MediaSense log levels table above for more information about debug and info message levels).
- Error-oraservice.<yyyy-MM-dd>T<HH-mm-ss.SSS>.startup.log: contains only system conditions.

Each of these files has a default maximum file size of 50 Megabytes (MB). The log file size and the number of files are not configurable.

Trace flags

Each service component has different logical divisions with corresponding trace flags. To ensure that a minimum level of logging information is captured whenever an issue occurs, a specific set of trace flags is enabled by default when MediaSense is installed. For the trace flags to take effect, you must set the log level for the corresponding component to DEBUG. Hence, the log level for most components is set to DEBUG by default when the MediaSense system is installed.

You can enable the entire component or certain trace flags within each component. You can also set different log level values (info or debug) for different MediaSense services in the same cluster.

MediaSense serviceability administration lists each trace flag within its MediaSense service component.

Caution You cannot create a trace file for the media service because this service does not support dynamic trace-level changes.

The list show the components that have their required trace flags enabled by default:

- MediaSense API service:
  - AMS system
  - Entering and exiting methods
  - SIP Adapter
- MediaSense call control service:
  - DEBUG
- MediaSense configuration service:
  - Configuration service data adapter

- Configuration service core
- Configuration service AXL interface
- System
- Configuration notification

- MediaSense serviceability administration:
  - System activities
  - Configuration service interaction
  - System service interaction
  - Audit information
  - Clustering activities
  - Controller class activities

- MediaSense administration:
  - Administration service core
  - DB access
  - General ORA administration user interface
  - Administration configuration update
  - Administration utilities

- MediaSense storage management agent:
  - DEBUG

Trace file location

The trace file contains information about each service.

After configuring the information that you want to include in the trace files for each service, you can collect and view the trace files by using the Unified Communications Trace and Log Central option in the Unified Real-Time Monitoring Tool (Unified RTMT). Trace and Log Central is the Unified Communications component which manages and provides access to trace files. When the services start up (during the post-installation process), the trace and log files are visible in the RTMT Trace and Log Central section after you launch Unified RTMT.

See *Cisco Unified Real-Time Monitoring Tool Administration Guide* (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html) for detailed information.

Set up trace file information

Caution By default, trace flags are set for each component to collect the minimum amount of information in case an issue arises. These flags are selected based on their value in capturing the most information without impacting the performance of the system. In some cases, you may need to enable additional trace flags (usually under the direction of Cisco Support to collect more information in the logs for an issue). These additional trace flags may slow performance of the system. If that is the case, after the information is collected, disable these additional trace flags.

To configure trace file information and to enable and disable trace flag settings, follow this procedure.

Procedure

Step 1 From MediaSense Serviceability Administration select **Trace** > **Configuration**.
The Trace Configuration web page opens displaying the configured trace flags along with the applicable trace flags for each service.

Step 2 For each service, select the required trace log levels and trace flags.

Step 3 Click **Save** to generate the trace files per the configured settings.
Alternately, click **Reset** to revert to the default settings for the selected service or click **Cancel** to revert to your previous settings.

Step 4 Retrieve the saved file from the corresponding trace file location.

Trace file interpretation

The MediaSense server stores the trace files in a log folder within the folder in which you installed the MediaSense component. You can collect and view trace information using Unified RTMT.

Performance logging

Use the performance logging web page to configure thread traces and memory traces so that you can monitor the performance of MediaSense clusters.

From the performance logging web page, you can dump thread and memory traces for the following MediaSense services:

- API service
- Configuration service
- Call control service
- Storage management agent
- Administration
- Diagnostics
- Serviceability administration

- System service
- Perfmon agent

Each trace dump provides varied log information in different log files:

- The dump thread trace feature provides log information about all threads for each service (name, state, and stack) in the following four-part (.txt) file name format:

  ```
  diagnostic-threads.<process-id>.<service-id>.<time stamp>.txt
  ```

- The dump memory trace feature provides memory information for each service in the following four-part (.hprof) file name format:

  ```
  diagnostic-memory.<process-id>.<service-id>.<time stamp>.hprof
  ```

- The dump memory trace feature also provides heap information for each service in the following four-part (.txt) file name format:

  ```
  diagnostic-memory.<process-id>.<service-id>.<time stamp>.txt
  ```

When you dump trace information, the information for the selected service (thread or memory) is collected in the log folder for that service. You can then use the Unified Real Time Monitoring Tool (Unified RTMT) to download the log file.

Dump trace parameters

Procedure

Step 1 From MediaSense Serviceability Administration select **Trace** > **Performance Logging**.
The performance logging web page opens displaying the configured trace flags along with the list of applicable services.

Step 2 Select the service for which you need to collect the trace parameters.

Step 3 Click **Dump Thread Trace** to generate the thread trace files for the selected service. This dump option allows you to detect deadlocks and analyze whether a thread uses excessive resources or causes out-of-memory errors.
Alternately, click **Dump Memory Trace** to generate the memory trace files for the selected service. This dump option allows you to find objects which use a large amount of memory in the Java Heap.

This creates the corresponding log files in the folder for the selected service.

Step 4 Retrieve the saved file from the corresponding trace file location using Unified RTMT.

Serviceability tools

To troubleshoot a problem, you may need to manage services in MediaSense Serviceability and in Unified Serviceability.

See the *Cisco Unified Serviceability Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Control center network services

Control center network services are installed automatically.

After the installation, control center network services start automatically in each server in the cluster. You can stop these network services if necessary.

Note

- The local server time is displayed in the administration interface. This time cannot be configured.
- In MediaSense release 9.0(1) only, because SNMP is not supported, you cannot configure SNMP community strings in Unified Serviceability Administration. Configuring these strings will hang the host resources agent.

Manage network services

Use this information to start, stop, and restart network services.

Procedure

Step 1 From the MediaSense Serviceability menu bar, click **Tools** and select **Control Center - Network Services**. Services that display in the **Control Center - Network Services** window do not start until you start each service.

The Control Center - Network Services web page displays the configurable MediaSense services along with the service status for the default server (the primary server in the cluster).

Caution Like other network services, the system service and serviceability administration are operational at startup. You cannot stop the system service or MediaSense serviceability administration from this web page. If the system service or serviceability administration goes down, no service control operations can take place. If you encounter any problem with the system service or serviceability administration, you can start or restart these services using the utils service, on page 105 command.

Step 2 To start, stop, or restart services, check the check box preceding the required service name.
A check mark appears in the check box to indicate your selection.

Step 3 Click the **Start**, **Stop**, or **Restart** button to perform the required operation.
A progress message appears in the status section (below the toolbar) to indicate task completion or s corresponding error message.

Note At any time, click **Refresh** to update the screen with the latest status of the services.

Control center feature services

MediaSense serviceability provides several options to control feature services.

Manage feature services

Use this information to start, stop, or restart MediaSense feature services.

Procedure

Step 1 From the MediaSense Serviceability menu bar, click **Tools** and select **Control Center - Feature Services** . Services that display in the Control Center - Feature Services window do not start until you start each service.

The Control Center - Feature Services web page displays the configurable MediaSense services along with their status for the default server (the primary server in the cluster).

Step 2 To start, stop, or restart services, check the check box preceding the required service name.
A check mark appears in the check box to indicate your selection.

Step 3 Click the **Start**, **Stop**, or **Restart** button to perform the required operation.
A progress message appears in the status section (below the toolbar) to indicate task completion or a corresponding error message.

Note At any time, click **Refresh** to update the screen with the latest status.

Media service call control service or database service reactivation

Reactivating the media service, the call control service, or the database service results in the following consequences:

- The existing recordings before the restart will not be available after the reactivation.
- You can record new calls only after the service is reactivated.

Note Reactivate or restart call control, database, and media services during off-peak hours to ensure minimum disruption to recordings in progress.

Access serviceability user interface for other servers in cluster

Before You Begin

The MediaSense configuration service must be in the *In service* state in either the primary server or the secondary server so that the cluster details can be displayed in the Cluster Access web page.

Procedure

Step 1 From the MediaSense Serviceability menu bar, click **Tools** and select **MediaSense Cluster Access**.
The **Cisco MediaSense Cluster Access** web page displays the available links for each server in this cluster. Each server is identified as a primary server, a secondary server, or an expansion server. The corresponding

link takes you to MediaSense serviceability administration for this server. You must sign in to one of these servers to continue.

Step 2 In the MediaSense **Serviceability Administration Authentication** window, enter the User ID and password. Select **Sign in**.

Unified RTMT administration

This section provides details specific to MediaSense for the Unified Real-Time Monitoring Tool (Unified RTMT). The Unified RTMT tool, which runs as a client-side application, uses HTTPS and TCP to monitor system performance and device status for MediaSense. Unified RTMT can connect directly to devices using HTTPS to troubleshoot system problems.

Even when Unified RTMT is not running as an application on your desktop, tasks such as performance monitoring updates continue on the server in the background.

Caution The VLT plug-in is not available in MediaSense. The plug-in is not available because Cisco VLT does not support message files involving Session Initiation Protocol (SIP) calls.

Warning You can monitor a maximum of 3000 processes and threads in a MediaSense system. The *Maximum Number of Processes and Threads* field is required by Unified CM in the Unified OS. This field specifies the maximum number of processes and threads running on the server. If the total number of processes and threads exceeds 3000, an alarm and corresponding alert are generated. See the Unified CM documentation (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html) for more information.

Unified RTMT installation and setup

You can install Unified RTMT on a computer that is compatible with the MediaSense software. To install the Unified RTMT plug-in from MediaSense Administration, see Download the Unified RTMT plug-in, on page 83.

Note To obtain a complete list of supported hardware and software for MediaSense, see the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified Contact Center Enterprise* at: http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html.

Download the Unified RTMT plug-in

To download the Unified RTMT Plug-in, follow this procedure.

Procedure

Step 1 From the Cisco MediaSense Serviceability menu bar, click **Tools** and select **RTMT Plugin Download**.
The Unified RTMT Plugin Download web page is displayed.

Step 2 To download the Unified RTMT Plugin executable to the preferred location on the client machine, click **Download**.
Follow the download procedure to install Unified RTMT on your client.

Step 3 After the Unified RTMT welcome window appears, click **Next**.

Step 4 To accept the license agreement, check the box next to **I accept the terms of the license agreement** ; then, click **Next**.

Step 5 Choose the location where you want to install Unified RTMT. If you do not want to use the default location, click **Browse** and navigate to a different location. Click **Next.**

Step 6 To begin the installation, click **Next**.
The Setup Status window is displayed. Do not click Cancel.

Step 7 To complete the installation, click **Finish.**

Unified RTMT upgrade

Unified RTMT saves user preferences and downloaded module jar files locally on the client server. It also saves user-created profiles in the database. You can still access these items in Unified RTMT after you upgrade the tool.

Note To ensure compatibility, you must upgrade Unified RTMT after you complete the MediaSense administration upgrade on all servers in the cluster.

Unified RTMT multiple copy installations

You cannot install more than one copy of Unified RTMT on a server. That copy can monitor any Unified Communications product and any number of MediaSense clusters.

To monitor a product on a server in a different cluster, you must first log off the server before you can log on to the other server.

Server status monitoring

The Systems tab lists all critical services related to the system and the MediaSense tab defines all critical services related to MediaSense. These critical services are enabled when VOS starts.

Performance monitoring counters

Unified Communications provides performance monitoring (perfmon) counters that enable you to monitor MediaSense in real time. MediaSense maintains the values of its perfmon counters. Unified RTMT enables you to view the counter values.

See the *Cisco Unified Real-Time Monitoring Tool Administration Guide* (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html) for detailed information about the Unified RTMT user interface and its logs.

Unified RTMT for performance monitoring

The Unified RTMT tracks and displays current performance information and alerts for MediaSense. Unified RTMT is integrated with the MediaSense administration and serviceability software.

Unified RTMT enables you to monitor the performance of all servers in MediaSense clusters. You can also continuously monitor a set of pre-configured objects.

In addition, Unified RTMT:

- Sends pop-up or email alerts to system administrators when performance counter values exceed predefined thresholds.
- Saves and restores settings, such as counters being monitored, threshold settings, and alert notifications, so that you can customize troubleshooting tasks.
- Charts up to six Perfmon counter values so that you can compare them.

System condition and perfmon counter alerts

Unified RTMT displays both pre-configured alerts and custom alerts in Alert Central. Unified RTMT organizes the alerts under several tabs—System, Custom, and MediaSense. Although the System tab and Custom tab are the same as those tabs available in Unified CM, the MediaSense tab is specific to MediaSense.

In MediaSense, system conditions are used to interpret the working states of the system. Whenever an error or a critical situation arises that prevents the system from functioning at its maximum capacity, a system condition is raised to indicate the problem. When the problem is resolved, the system condition is cleared and the system returns to normal state. The system condition contains information about the problem and possible corrective actions to address the problem. The various MediaSense log messages can have a system condition which can be raised and cleared based on the log message.

System condition alerts and perfmon counter alerts for MediaSense are visible as individual alerts on the MediaSense tab in the Alert Central tool in Unified RTMT. Each alert description explains the system condition and possible actions to resolve it.

Items in red indicate that an alert has been raised. If the alert is cleared, the timestamp is updated by the alert. The timestamp remains red so that it is visible when the administrator signs in. In the Safe region, the *Yes* indicates that the alert was raised under normal conditions, and the *NA* indicates that the safe range field does not apply to the system condition.

The following table lists the system condition alerts (prepended by SC_) and perfmon counter alerts (prepended by PC_) and their corresponding descriptions within each MediaSense service class object.

Table 7: System condition and perfmon counter alerts

Service	Alert SC_ = system condition alert PC_ = perfmon counter alert	Description	Recommended action
Tomcat (config service)	SC_ConfigLostContactWithDB	The configuration service lost contact with its database service.	Check the MediaSense database service. Restart it if necessary.
	SC_ConfigurationOOS	The configuration service is out of service.	Check the MediaSense database service. Restart it if necessary.
	SC_ConfigurationLostContact WithAXL	The configuration service lost contact with its Unified CM AXL server.	Check the Unified CM AXL configuration. Modify or restart it if necessary.
MediaSense call control service	SC_RecordingLatencyWarning	Recording start latency exceeds warning threshold.	Check the media server. Restart it if necessary.
	SC_CallControlOOS	Call control service is out of service.	Check the call control server. Restart it if necessary.
	SC_CallControlLostContact WithAPI	Call control service lost contact with API Service.	Check the API server. Restart it if necessary.
	SC_CallControlLostContact WithMedia	Call control service lost contact with media Service.	Check the Media server. Restart if necessary.
	SC_CallControlLoadCritical	Call load exceeds critical threshold.	Reduce the load by decreasing the number of phones that are configured for recording in a given cluster or install an additional MediaSense server.
	PC_CallControlMaximumHeap Memory ThresholdReached	Safeguards the MediaSense system from running out of memory. If this counter crosses the 128 MB memory threshold, the system triggers an alert.	Reduce the load by decreasing the number of phones that are configured for recording in a given cluster or install an additional MediaSense server.

Service	Alert SC_ = system condition alert PC_ = perfmon counter alert	Description	Recommended action
Tomcat API service	SC_APILostContactWith Database	API Service lost contact with its database service.	Check the MediaSense database service. Restart it if necessary.
	SC_APIServiceOOS	API Service is out of service.	Check if SC_ORA_API_LOST_ CONTACT_WITH_ DATABASE has also been raised. If yes, then check the MediaSense database service. Restart it if necessary. If that does not work, restart Tomcat (API Service). If SC_ORA_API_LOST_ CONTACT_WITH_ DATABASE has not been raised, then restart Tomcat (API Service).
MediaSense system service	SC_SystemServiceOOS	The system service is out of service.	Check system service. Restart it if necessary.
MediaSense database service	SC_DatabaseServiceOOS	database service is out of service.	Check the database service. Restart it if necessary.
MediaSense storage management agent	SC_DiskSpaceWarning	Available media storage level is low.	Consider deleting old recordings.
	SC_DiskSpaceCritical	Available media storage level is critical. The system may fail to process new requests.	Delete old recordings to free up storage space.
	SC_DiskSpaceEmergency	No media storage space is available. This server is not functional.	Delete old recordings to free up storage space.

AMC service and Unified CM setup

To support the Unified RTMT client, a number of services must be active and running on the MediaSense server. AMC service is one such service. It starts up automatically after the Unified RTMT installation and

allows the Unified RTMT client to retrieve real-time information from the MediaSense server. The AMC service, the Alert Manager, and the collector service enable Unified RTMT to retrieve real-time information from the server or from all servers in the MediaSense cluster.

To view the state of the AMC service, navigate to Unified CM Administration on MediaSense server and choose **System** > **Service Parameters**. Then, choose the required server and select the **Cisco AMC service** . For more information about the AMC Service, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* (http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html).

Caution If for any reason, the primary MediaSense server shuts down or is in a failed state, and the secondary MediaSense server continues to function in the normal state. If you launch the Unified RTMT client at this time, the MediaSense tab in the Alert Central window may remain blank and display `Error polling alert \ status. AMC service is down.` in the status pane. Similarly, the System Summary pane may display `HTTP request failed. Web Server unreachable.` for the same issue. To work around this issue, configure the secondary Cisco AMC Service **in the primary Cisco MediaSense server**.

Note Be sure to make the following change in the **primary Cisco MediaSense server** first.

Navigate to Unified CM Administration (in **the primary Cisco MediaSense server**). Choose **System** > **Service Parameters**. Then, select the secondary MediaSense server from the drop-down list, and finally select **Cisco AMC Service**. In the resulting Service Parameter Configuration web page, select the secondary MediaSense server from the drop-down list next to the **Failover Collector** field. After you configure the AMC Service for the secondary MediaSense server, the secondary server takes over when the primary MediaSense server goes down, and Unified RTMT continues to display alert names under Alert Central.

Note You can access Unified CM Administration on the MediaSense server by providing the following URL format in a browser window: `http://<MediaSenseServer-ip-address>/ccmadmin`.

Trace and log central Unified RTMT setup

The trace and log central feature in Unified RTMT enables you to configure on-demand trace collection for a specific date range or for an absolute time. You can collect trace files that contain the search criteria that you specify. You can also save the trace collection criteria for later use, schedule one recurring trace collection and download the trace files to a SFTP or FTP server on your network, or collect a crash dump file. After you collect the files, you can view them in the appropriate viewer within Unified RTMT. You can also view traces on the server without downloading the trace files by using the remote browse feature. You can open the trace files by either selecting the internal viewer that is provided with Unified RTMT or selecting another appropriate application as an external viewer.

Note To use the trace and log central feature in Unified RTMT, make sure that Unified RTMT can directly access all servers in the cluster without using Network Access Translation (NAT).

File collection

The collect files tool allows you to specify the required MediaSense services and application in the **Select MediaSense Services/Application** tab, which is part of the collect files wizard. After you specify the required MediaSense services, continue to proceed as you would for the System Service/Application. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use.

Crash dump collection

Unified Serviceability stores the logs for the version of application that you are logged in to in the active partition and stores the logs for the other version (if installed) in the inactive folder.

Remote browse folder names and services

To view .log or .out files, use one of the following applications:

- Right-click the required file and select **Open** to view it in the Default Viewer.
- Right-click on the required file and select **Open with** to view all available applications with which to view these files.

Caution MediaSense does not support the QRT Viewer.

The remote browse folder name (log and trace file folder name) for each MediaSense service is shown in the second column of the following table.

MediaSense service or agent name	Remote browse folder name
Call control service	callcontrol
Media service	media
API service	ora
Configuration service	oraconfiguration
Database service	oradb
SM agent	storagemanagementagent
MediaSense administration	oraadmin
Serviceability administration	oraservice
System service	systemservice
Perfmon agent	perfmonagent
Diagnostics	diagnostics

Caution MediaSense provides some log files in a GZIP format. However, in Unified RTMT, the trace and log central remote browse feature does not display these files by default. You can add the appropriate application or download and save the .gzip file and view it directly from the downloaded location.

Perfmon agent and counters

The perfmon agent monitors performance for MediaSense. It has no separate user interface. It operates seamlessly within MediaSense serviceability administration. Like other network services, the perfmon agent is operational at startup.

The perfmon agent retrieves its performance monitoring counter values from JMX MBeans and writes these values to the Unified Communications Manager database.

The perfmon agent also logs the perfmon counter values in the Unified RTMT. You can use Unified RTMT to view the most recent counter values and descriptions and to identify the objects that are available for system monitoring.

The following table classifies, names, and describes perfmon counters. The first column shows perfmon counters by class and name. The second column contains the counter descriptions. Note that the class objects provide process or time-usage information in percentages.

Counter class and name	Counter description
Class: MediaSense call control service	
Recording sessions counters	
Heap memory usage	Sends an alert when its value exceeds 128 MB of memory (to help keep MediaSense from running out of memory).
Number of active sessions	The number of active recording sessions.
Number of recorded sessions without errors	The number of recorded sessions completed without errors.
Number of recorded sessions with errors	The number of recorded sessions completed with errors.
Recording setup time	
Mean setup delay	The average delay (in milliseconds) between the initial receipt of the SIP Invite from Unified CM and the SIP response to the Unified CM rolling window time.
Max setup delay	The maximum delay (in milliseconds) between the initial receipt of the SIP Invite from Unified CM and the SIP response to the Unified CM rolling window time.
Stream dialog API (used by video greeting in Unity Connection)	

Counter class and name	Counter description
Started dialogs	The total number of stream dialogs started.
Start record API requests	The total number of successfully started stream dialog start recording requests.
Start playback API requests	The total number of successfully started stream dialog start playback requests.
Rejected dialogs due to busy	The total number of stream dialog start requests that returned BUSY.
Mean start record time	The average amount of time (in milliseconds) taken to successfully start a recording operation.
Mean start playback time	The average amount of time (in milliseconds) taken to successfully start a play operation.
Mean dialog time	The average amount of time (in milliseconds) a stream dialog was active.
Max start record time	The maximum amount of time (in milliseconds) taken to successfully start a recording operation.
Max start playback time	The maximum amount of time (in milliseconds) taken to successfully start a play operation.
Max dialog time	The maximum amount of time (in milliseconds) a stream dialog was active.
Completed dialogs	The total number of stream dialogs completed.
Average active dialogs on busy	The average number of stream dialogs (rounded down to nearest integer) that were active when a stream dialog start request returned BUSY.
Class: MediaSense media service	
Number of active playbacks	The number of outgoing RTSP sessions.
Number of live monitored calls	The number of ports used for live-monitored calls. One live-monitored call uses two ports in most cases.
Class: MediaSense configuration service	
Authentication request processing: average latency	The average latency for processing an authentication request.
Authentication request processing: max latency	The maximum latency for processing an authentication request.

Counter class and name	Counter description
Total requests	For Cisco use only.
Total failures	The total number of request failures encountered by the MediaSense configuration service.
Class: MediaSense API service	
Mean query response time	The average query response time in the last hour.
Max query response time	The maximum query response time in the last hour.
Total number of responses	The total number of successful and unsuccessful responses.
Total number of requests	The total number of requests received and serviced by the API Service.
Avg time per request	The average time for each request received and serviced by the Call Control Service in the last hour.
Max time per request	The maximum time for each request received and serviced by the Call Control Service in the last hour.
Max number of concurrent requests	The maximum number of concurrent requests received and serviced by the Call Control Service in the last hour.
Total number of concurrent requests in progress	The total number of concurrent requests in progress in the last hour.
Class: MediaSense SM agent	
Common partition usage	The percentage of common partition disk usage.
Media # partition usage	The percentage of disk usage of each media partition.
Audio recording ports in use	The number of audio ports currently in use for recording.
Video recording ports in use	The number of video ports currently in use for recording.
Available audio ports	The number of audio ports available.
Available video ports	The number of video ports available.
Total audio ports in use	The number of audio ports currently in use.
Total video ports in use	The number of video ports currently in use.
Total RTSP playback requests	The number of RTSP playback requests.

Counter class and name	Counter description
Total RTSP playback requests last 5 min.	The number of RTSP playback requests in the last 5 minutes.
Rejected RTSP playback requests	The number of rejected RTSP playback requests
Rejected RTSP playback requests last 5 min.	The number of rejected RTSP playback requests in the last 5 minutes.
Total RTSP monitoring requests	The number of RTSP monitoring requests
Total RTSP monitoring requests last 5 min.	The number of RTSP monitoring requests in the last 5 minutes.
Rejected RTSP monitoring requests	The number of rejected RTSP monitoring requests.
Rejected RTSP monitoring requests last 5 min.	The number of rejected RTSP monitoring requests in the last 5 minutes.
Total raw download requests	The number of raw download requests
Total raw download requests last 5 min.	The number of raw download requests in the last in 5 minutes.
Rejected raw download requests	The number of rejected raw download requests.
Rejected raw download requests last 5 min.	The number of rejected raw download requests in the last 5 minutes.
Total convert requests	The number of convert requests.
Total convert requests last 5 min.	The number of convert requests in the last 5 minutes.
Rejected convert requests	The number of rejected convert requests.
Rejected convert requests last 5 min.	The number of rejected convert requests in the last 5 minutes.
Class: MediaSense database service	
This class has no perfmon counters.	
Class: MediaSense system service	
This class has no perfmon counters.	
Class: MediaSense diagnostics	
This class has no perfmon counters.	

Counter class and name	Counter description
Class: MediaSense administration	
This class has no perfmon counters.	
Class: MediaSense serviceability administration	
This class has no perfmon counters.	

Server IP address changes

Use the following procedures to change the IP address of any fully installed server in a MediaSense cluster (meaning that the setup wizard must have finished running on the server for which the IP address is being changed).

Note Do not attempt to change the IP address of any server while another server is being installed. Use these procedures only on a fully installed server (do not attempt to use these procedures if an installation has failed or while installation is in progress on any server in the cluster.

Prepare system for IP address change

Perform the following tasks to ensure that your system is prepared for a successful IP address change.

Procedure

Step 1 List all servers in the cluster and note whether the servers are defined by using IP addresses or by host names.

- If you are verifying the list from the MediaSense Administration interface on the primary server, navigate to **System** > **MediaSense Server Configuration**. A list of all servers in the cluster is displayed.
- If you are verifying the list from the command line interface (CLI) on the primary server, issue the **Show Network Cluster** command.

a) Capture the details of this list for later reference.

Step 2 Save a list of the hostname and IP address of each server in the cluster.

Step 3 Ensure that all servers in the cluster are running and available by checking for any active ServerDown alerts. You can check from the Unified RTMT interface or from the CLI on the primary server.

- To check from the Unified RTMT interface, access Alert Central and check for ServerDown alerts.
- To check from the CLI on the primary server, issue the `file search activelog syslog/CiscoSyslog ServerDown` command and inspect the application event log.

Step 4 Check the database replication status on all MediaSense servers in the cluster to ensure that all servers are replicating database changes successfully.
You can check by using the Unified RTMT interface or a CLI command.

- Unified RTMT interface: access the database summary and inspect the replication status.
- CLI: Enter the command shown in the following example:

```
show perf query class "Number of Replicates Created and State of Replication"
==>query class:
- Perf class (Number of Replicates Created and State of Replication)
has instances and values:
ReplicateCount  -> Number of Replicates Created   = 344
ReplicateCount  -> Replicate_State                = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case.

The following list shows the possible values for Replicate_State:

- 0 = Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service has not been running since subscriber installed.
- 1 = Replicates have been created, but their count is incorrect.
- 2 = Replication is good.
- 3 = Replication is bad in the cluster.
- 4 = Replication setup did not succeed.

Step 5 To check for network connectivity and DNS server configuration, enter the `utils diagnose module validate_network` command.

Example:

```
utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log
Starting diagnostic test(s)
===========================
test - validate_network: Passed
Diagnostics Completed
```

Change IP address of primary server

Warning Using this procedure disrupts all services. Be sure to use it only during a scheduled downtime.

Use this procedure to change the IP address of a MediaSense primary server if your cluster servers are defined using host names. To successfully change the IP address, you must complete all steps in this procedure.

Procedure

Step 1 Review and address the instructions listed in Prepare system for IP address change, on page 94 before changing the IP address on any MediaSense server.

Step 2 Verify that the DNS change propagates to other servers by using the `utils network host` and `show tech network hosts` CLI commands on all servers in the cluster.

Example:

```
utils network host mcs-sec
Hostname mcs-sec resolves to 10.10.10.136

show tech network hosts
-------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed
from the cluster.
127.0.0.1 localhost
1 10.10.10.92 mcs-pri.cisco.com mcs-pri
2 10.10.10.93 mcs-sec.cisco.com mcs-sec
3 10.10.10.137 mcs-exp1.cisco.com mcs-exp1
```

Step 3 From the *primary* server, issue the `set network cluster server ip` command to update the MediaSense cluster configuration with the primary server's new IP address.

Example:

```
set network cluster server ip 10.10.10.92 10.10.10.135
Setting server ip 10.10.10.92 10.10.10.135
Successful
```

Step 4 Verify the interim cluster configuration by issuing the `show network cluster` command.

Example:

```
show network cluster
1 10.10.10.135 mcs-pri Primary not authenticated or updated on server
2 10.10.10.93 mcs-sec.cisco.com mcs-sec Secondary authenticated using TCP since Mon Sep 12
 12:33:16 2011
3 10.10.10.137 mcs-exp1.cisco.com mcs-exp1 Expansion authenticated using TCP since Mon Sep
 12 12:33:06 2011
- 10.194.118.92 mcs-pri.cisco.com mcs-pri Primary authenticated
```

Step 5 Point every server in the cluster to the new primary's IP address by issuing the `set network cluster primary ip` command from each server in the MediaSense cluster, including the primary server:

Example:

```
set network cluster primary ip 10.10.10.135
Setting primary ip to 10.10.10.135
Successful
```

Step 6 Ensure that the IP address change is replicated to the secondary and expansion servers database by entering the `run sql select name,nodeid from ProcessNode` command on all servers in the cluster. The following example shows the command output:

Example:

```
run sql select name,nodeid from ProcessNode
name                 nodeid
==================== ======
EnterpriseWideData 1
mcs-pri            2
mcs-sec            3
mcs-exp1           4
```

Step 7 If you are moving the primary server to a different subnet that requires a new default gateway address, change the default gateway by issuing the `set network gateway` command from the *primary* server:

Example:

```
set network gateway 10.3.90.2
***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
```

Note If you change the default gateway, you may also need to change the subnet mask. See the Unified OS documentation for further details.

Step 8 From the *primary* server, issue the `set network ip eth0` command to reset the network adapter to the new IP address.

Example:

```
set network ip eth0 <server new ip> <address mask> <gw>
set network ip eth0 10.194.118.137.92 255.255.255.0 10.194.118.1

***   W A R N I N G   ***
You must first change the IP Address using the
<set network cluster server> CLI command BEFORE
changing it here or call recording will fail.
This will cause the system to restart.

=======================================================
Note: To recognize the new IP address all nodes within
the cluster must be manually rebooted.
=======================================================
Continue (y/n)? y
```

This command changes the IP address and re-boots the primary server.

Step 9 Type **Yes** and press **Enter**.

Step 10 To update the local name resolution files, reboot all other servers in the cluster . Include hosts, rhosts, sqlhosts, and services.

Note Server restart ensures the proper update and service-restart sequence for the IP address changes to take effect.

Step 11 Verify that the DNS change propagates to other servers by using the `utils network host` and `show tech network hosts` commands on all servers in this cluster.

Example:

```
utils network host mcs-pri
Hostname mcs-pri resolves to 10.10.10.135
```

```
show tech network hosts
-------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
1 10.10.10.135 mcs-pri.cisco.com mcs-pri
2 10.10.10.93 mcs-sec.cisco.com mcs-sec
3 10.10.10.137 mcs-exp1.cisco.com mcs-exp1
```

Step 12 Verify the cluster configuration by issuing the `show network cluster` command.

Example:

```
show network cluster
1 10.10.10.135 mcs-pri.cisco.com mcs-pri Primary
authenticated using TCP since Mon Sep 12 14:43:59 2011
2 10.10.10.93 mcs-sec.cisco.com mcs-sec Secondary authenticated
3 10.10.10.137 mcs-exp1.cisco.com mcs-exp1 Expansion
authenticated using TCP since Mon Sep 12 14:44:05 2011
```

Caution It may take some time for the cluster to synchronize the new IP address information. During this time, the output for this command may show partial or incomplete information.

Change IP address of secondary server

Warning This procedure disrupts all services. Be sure to make any changes during a scheduled downtime.

Use this procedure to change the IP address of a MediaSense secondary server if your cluster servers are defined using host names. To successfully change the IP address, you must complete all steps in this procedure.

Procedure

Step 1 Review and address the instructions listed in Prepare system for IP address change, on page 94 before changing the IP address on any MediaSense server.

Step 2 From the *primary* server, issue the **set network cluster server** command to update the MediaSense cluster configuration with the secondary server's new IP address.

Example:

```
set network cluster server ip 10.10.10.93 10.10.10.136
Setting server ip 10.10.10.93 10.10.10.136
Successful l
```

Step 3 Verify the interim cluster configuration by issuing the **show network cluster** command.

Example:

```
show network cluster

1 10.10.10.135 mcs-pri.cisco.com mcs-pri Primary
```

```
  authenticated using TCP since Mon Sep 12 12:53:16 2011
2 10.10.10.136 mcs-sec Secondary not authenticated or updated on server
3 10.10.10.137 mcs-exp1.cisco.com mcs-exp1 Expansion
  authenticated using TCP since Mon Sep 12 12:53:06 2011
  - 10.194.118.93 mcs-sec.cisco.com mcs-sec Secondary authenticated
```

Step 4 Point every server in the cluster to the new secondary server IP address by issuing the **set network cluster secondary ip** command:

Example:

```
set network cluster secondary ip 10.10.10.136
Setting secondary  ip to 10.10.10.136
Successful
```

Step 5 If you are moving the secondary server to a different subnet that requires a new default gateway address, change the default gateway by issuing the **set network gateway** command from the *secondary* server:

Example:

```
set network gateway 10.3.90.2
***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
```

Step 6 Type **Yes** and press **Enter**.

Step 7 Ensure that the IP address change is replicated to the secondary and expansion server databases by entering the **run sql select name,nodeid from ProcessNode** command on all servers in the cluster. The following example shows the command output:

Example:

```
run sql select name,nodeid from ProcessNode
name                nodeid
=================== ======
EnterpriseWideData 1
mcs-pri            2
mcs-sec            3
mcs-exp1           4
```

Step 8 From the *secondary* server, issue the **set network ip eth0 <server new ip> <address mask> <gw>** command to set the network adapter to the new IP address.

Example:

```
set network ip eth0 10.194.118.137 255.255.255.0 10.194.118.1

***   W A R N I N G   ***
You must first change the IP Address using the
<set network cluster server> CLI command BEFORE
changing it here or call recording will fail.
This will cause the system to restart
=======================================================
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
```

```
============================================================
Continue (y/n)? y
```

Step 9 Re-boot all servers in the MediaSense cluster to update the local name resolution files. Include the hosts, rhosts, sqlhosts, and services.

Note Restarting the server ensures that changes occur in proper order for the update and service-restart sequence for the IP address.

Step 10 Verify that the DNS change propagates to other servers by using the **utils network host** command and the **show tech network hosts** command on all servers in this cluster.

Example:

```
utils network host mcs-sec
Hostname mcs-sec resolves to 10.10.10.136

show tech network hosts
-------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
1 10.10.10.135 mcs-pri.cisco.com mcs-pri
2 10.10.10.136 mcs-sec.cisco.com mcs-sec
3 10.10.10.137 mcs-exp1.cisco.com mcs-exp1
```

Step 11 Verify the interim cluster configuration by issuing the **show network cluster** command.

Example:

```
1 10.10.10.135 mcs-pri.cisco.com mcs-pri Primary authenticated using TCP
               since Mon Sep 12 14:43:59 2011
2 10.10.10.136 mcs-sec.cisco.com mcs-sec Secondary authenticated
3 10.10.10.137 mcs-exp1.cisco.com mcs-exp1 Expansion
               authenticated using TCP since Mon Sep 12 14:44:05 2011
```

Change IP address of expansion server

Warning This procedure disrupts all services. Make any changes only during a scheduled downtime.

If your cluster servers are defined using host names, use this procedure to change the IP address of any expansion servers. To successfully change the IP address, you must complete all steps in this procedure.

Procedure

Step 1 Review and address the instructions listed in Prepare system for IP address change, on page 94 before changing the IP address on any server.

Step 2 From the CLI of the *primary* server, issue the `set network cluster server ip` command to update the cluster configuration with the new IP address of the expansion server.

Example:

```
set network cluster server ip 10.10.10.100 10.10.10.137
```

```
Setting server ip 10.10.10.100 10.10.10.137
Successful
```

Step 3 Verify the interim cluster configuration by issuing the `show network cluster` command.

Example:

```
show network cluster
1 10.10.10.92 mcs-pri.cisco.com mcs-pri Primary authenticated
2 10.10.10.93 mcs-sec.cisco.com mcs-sec Secondary
              authenticated using TCP since Fri Sep 9 08:52:50 2011
3 10.10.10.137 mcs-exp1 Expansion not authenticated or updated on server
               - 10.10.10.100 mcs-exp1.cisco.com mcs-exp1 Expansion
               authenticated using TCP since Fri Sep 9 11:40:34 2011
```

Step 4 Ensure that the IP address change is replicated to the secondary and expansion server databases by issuing the `run sql select name,nodeid from ProcessNode` command on all servers in the cluster. The following example shows the command output:

Example:

```
run sql select name, nodeid from ProcessNode
name                 nodeid
==================== ======
EnterpriseWideData 1
mcs-pri            2
mcs-sec            3
mcs-exp1           4
```

Step 5 If you are moving the expansion server to a different subnet that requires a new default gateway address, change the default gateway by issuing the `set network gateway` command from the *expansion* server:

Example:

```
set network gateway 10.3.90.2

***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
```

Step 6 From the *expansion* server, issue the `set network ip eth0 <server new ip> <address mask> <gw>` command to change the IP address of the expansion server.

Example:

```
set network ip eth0 10.194.118.137 255.255.255.0 10.194.118.1

***   W A R N I N G   ***

You must first change the IP Address using the
<set network cluster server> CLI command BEFORE
changing it here or call recording will fail.
This will cause the system to restart
======================================================
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
======================================================
Continue (y/n)? y
```

This command changes the IP address and re-boots the expansion server.

Step 7 Type **Yes** and press Enter.

Step 8 To update the local name resolution files, reboot all other servers in the cluster. Include all hosts, rhosts, sqlhosts, and services.

Note Restarting the server ensures the proper update and service-restart sequence for the IP address changes to take effect.

Step 9 Verify that the DNS change propagates to other servers by using the `utils network host` and `show tech network hosts` commands on all servers in this cluster.

Example:

```
utils network host mcs-exp1
Hostname mcs-exp1 resolves to 10.10.10.137

show tech network hosts
-------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
1 10.10.10.92 mcs-pri.cisco.com mcs-pri
2 10.10.10.93 mcs-sec.cisco.com mcs-sec
3 10.10.10.137 mcs-exp1.cisco.com mcs-exp1
```

Step 10 Verify the cluster configuration by issuing the `show network cluster` command.

Example:

```
show network cluster
1 10.10.10.92 mcs-pri.cisco.com mcs-pri Primary authenticated
2 10.10.10.93 mcs-sec.cisco.com mcs-sec
              Secondary authenticated using TCP since Mon Sep 12 12:33:16 2011
3 10.10.10.137 mcs-exp1.cisco.com mcs-exp1 Expansion
              authenticated using TCP since Mon Sep 12 12:33:06 2011
```

Change multiple IP addresses in a MediaSense cluster

Use this procedure to sequentially change the IP addresses for multiple MediaSense servers. If you use this procedure, you need to issue a series of commands **sequentially** and reboot only once. To successfully change the IP address for all servers in a cluster, you must complete all steps in this procedure.

Note This example procedure is written for a three-server cluster. As long as you change the IP addresses on one server at a time, you can modify this procedure for four-server or five-server clusters.

Caution Change an IP address on **only one server** at a time. Changing an IP address on more than one server at the same time may cause .hosts files and .sqlhosts files to become out-of-sync.

Warning Make changes only during a scheduled downtime. Changing IP addresses disrupts all MediaSense services.

Procedure

Step 1 Review the instructions in Prepare system for IP address change before changing the IP address on any MediaSense server.

Step 2 From the *primary* server, issue the following commands:

Example:

```
set network cluster server ip <primary current ip> <primary new ip>
set network cluster server ip <secondary current ip> <secondary new ip>
set network cluster server ip <expansion current ip> <expansion new ip>
set network cluster primary ip <primary new ip>
set network cluster secondary ip <secondary new ip>
```

Step 3 From the *secondary* server, issue the following commands:

Example:

```
set network cluster primary ip <primary new ip>
set network cluster secondary ip <secondary new ip>
```

Step 4 From the *expansion* server, issue the following commands:

Example:

```
set network cluster primary ip <primary new ip>
set network cluster secondary ip <secondary new ip>
```

Step 5 From the *primary* server, issue the following commands:

Example:

```
run sql select name,nodeid from ProcessNode
```

Step 6 From the *secondary* server, issue the following commands:

Example:

```
run sql select name,nodeid from ProcessNode
```

Step 7 From the *expansion* server, issue the following commands:

Example:

```
run sql select name,nodeid from ProcessNode
```

Step 8 From the *primary* server, issue the following commands:

Example:

```
set network gateway (if required)
set network ip eth0 <primary new ip> <address mask> <gw>
```

Step 9 From the *secondary* server, issue the following commands:

Example:

```
set network gateway (if required)
set network ip eth0 <secondary new ip> <address mask> <gw>
```

Step 10 From the *expansion* server, issue the following commands:

Example:

```
set network gateway (if required)
set network ip eth0 <expansion new ip> <address mask> <gw>
```

Step 11 From each server in the MediaSense cluster, issue the following commands to verify the cluster configuration.

Example:

```
utils network host
show tech network hosts
show network cluster
```

MediaSense command line interface (CLI) commands

MediaSense Administration is enabled for sign-in at the completion of the installation and is the primary interface for administering, configuring, and maintaining MediaSense. If MediaSense Administration is not accessible for any reason, you can use the CLI commands specified in this chapter to perform certain tasks.

In the command syntax descriptions:

- **Bold** is used for the base command.
- *Italics* are used for mandatory parameters when the syntax includes them.
- [brackets] are used for options when the syntax includes them.

MediaSense does not support any Platform CLI commands that are not specifically listed in this document.

CLI access

You can access the CLI as follows:

- Directly, using the monitor and keyboard at the VM console.
- Using SSH.

Procedure

Step 1 At either the sign-in prompt or the SSH client, enter the MediaSense administrator ID (created during the installation of the primary server).

Step 2 When prompted, enter the MediaSense administrator password.

You can start entering commands at the next prompt.

In addition to the CLI commands listed in the *Command Line Interface Reference Guides* and this chapter, you can also enter the following commands:

- **help**: To display the list of all supported commands. For example, to display help for a specific command, type `help utils service list` and press Enter.
- **quit**: To close the CLI.

Utils commands

The section provides details about the MediaSense-specific **utils** commands.

utils media recording_sessions

The **utils media recording_sessions** *file fileName* command generates an html file with a detailed list of the last 100 recording sessions processed by this MediaSense server. Confirm that the MediaSense call control service is running for before you execute this command. The file is saved to the platform/cli/ folder and can be downloaded using the `file get activelog platform/cli/fileName` command.

Command: **utils media recording_sessions** *file fileName*

Details:

- *file* is a mandatory parameter that outputs the information to a file.
- *fileName* is a mandatory parameter that defines the name of the .html file.
- When you issue this command, you get the following response:

```
MediaSense Call Control Service Recording sessions saved to platform/cli/<filename>.html
You can now download it using: file get activelog platform/cli/<filename>.html
```

  You can then retrieve the file from that directory and save it to a location of your choice.

Example:

- `utils media recording_sessions file sessions.html`

```
MediaSense Call Control Service Recording sessions saved to platform/cli/sessions.html
You can now download it using: file get activelog platform/cli/sessions.html
```

utils service

Purpose: Lists, starts, stops, or restarts each of the MediaSense services.

Command: **utils service** *operation service_name*

Details:

- *operation* specifies the type of operation to be performed by this command:

Valid operations include:

- *start*
- *stop*
- *restart*
- *list*

- *service_name* specifies the name of the MediaSense service for which you require the specified operation.

  Valid services include:

  - *MediaSense Administration*
  - *MediaSense Configuration Service*
  - *MediaSense Database Service*
  - *MediaSense Perfmon Agent*
  - *MediaSense System Service*
  - *MediaSense Diagnostics*
  - *MediaSense API Service*
  - *MediaSense Call Control Service*
  - *MediaSense Media Service*
  - *MediaSense Storage Management Agent*

Examples:

- `utils service list`
- `utils service start MediaSense Configuration Service`

utils system maintenance

The command **utils system maintenance** *operation* enables or disables maintenance mode on MediaSense or displays the MediaSense maintenance mode status. While it is in maintenance mode, MediaSense cannot process any recording or API requests.

MediaSense re-boots when it enters maintenance mode. Any streaming activities end abruptly. Any active recordings end in a CLOSED_ERROR state. MediaSense re-boots again when maintenance mode is disabled and it re-enters normal mode.

Command: **utils system maintenance** *operation*

Details: *operation* specifies what the command does.

Valid operations include:

- *enable*
- *disable*

- *status*

Examples:

- `utils system maintenance enable`
- `utils system maintenance disable`
- `utils system maintenance status`

Run commands

The section provides details about the MediaSense-specific **run** commands.

run db_reset_replication

Use this command to begin the process to manually reset replication for the entire MediaSense database. After the reset process is complete, this command returns a message with the status of the reset. You may need to use this command if the primary server fails within a multi-node cluster.

Note In a multi-server deployment, you can run this command only on the secondary server.

Command: **run db_reset_replication**

Details: This command has no options.

Example:

```
run db_reset_replication
```

run db_synchronization

Use this command to compare the databases in the primary and secondary servers to ensure that the databases are synchronized.

Note In a multi-server deployment, you can run this command only on the secondary server.

Command: **run db_synchronization** *database_name*

Details:

- *database_name* specifies the type of operation to be performed by this command.

  The valid database names are:

  - *db_ora_config*
  - *db_ora_meta*

Examples:

- `run db_synchronization db_ora_config`
- `run db_synchronization db_ora_meta`

Set network commands

The section provides details about the MediaSense-specific **set network** commands.

set network cluster server ip

This command updates the MediaSense cluster configuration with the new IP address of a specific server. It does not change the IP address of the server itself. Issue this command on the primary MediaSense server only. Issuing this command on any other server results in an error.

Caution This command may impact the synchronization of MediaSense services. Issue this command only as a part of the IP address change procedure. The MediaSense services may not be functional until the IP address change procedure is completed.

Note This command requires the Configuration Service to be reachable and running on the primary server.

You have three options to issue this command. In each case, the CLI reports a success or error as applicable.

- **With no arguments:** If you issue this command without any arguments, the CLI displays the list of servers. Select the server to be changed by entering the required number from the list index. (At this point, you can also quit by typing `q`.) You are then prompted to enter the new IP address of the server.
- **With one argument:** Provide the current IP address or the hostname of the server to be changed. The CLI prompts you to enter the new IP address of the server.
- **With both arguments:** Provide the current IP address or the hostname of the server to be changed and then provide the new IP address of the server.

- Command privilege level: 1
- Allowed during upgrade: Yes

Command: **set network cluster server ip** *current_host new_ip*

Details:

- *current_host* is the IP address or hostname of the server to be changed
- *new_ip* is the new IP address for the server

Examples:

- set network cluster server ip
  1) mcs-vm92 (1.1.1.92)
  2) 1.1.1.93
  3) mcs-vm100 (1.1.1.100)
  Enter server to change (1-3, 'q' to quit): 3
  Enter new IP address for mcs-vm100 (1.1.1.100): 1.1.1.137
  Setting server ip mcs-vm100 (1.1.1.100) to 1.1.1.137
  Successful
- set network cluster server ip mcs-vm100
  Enter new IP address for mcs-vm100 (1.1.1.100): 9.9.9.9
  Setting server ip mcs-vm100 (1.1.1.100) to 9.9.9.9
  Successful
- set network cluster server ip 1.1.1.100 9.9.9.9
  Setting server ip mcs-vm100 (1.1.1.100) to 9.9.9.9
  Successful

set network cluster primary ip

This command configures the primary server IP address mapping in a given server.

Caution This command may impact the synchronization of MediaSense services. Issue this command only as a part of the IP address change procedure. The MediaSense services may not function until the IP address change procedure is completed.

- Command privilege level: 1
- Allowed during upgrade: Yes

Command: **set network cluster primary ip** *new_ip*

Detail: *new_ip* is the new IP address for the primary server

Example:

```
set network cluster primary ip 9.9.9.9
Setting primary ip to 9.9.9.9
Successful
```

set network cluster secondary ip

This command configures the secondary server IP address mapping in a given server.

Caution This command may impact the synchronization of MediaSense services. Issue this command only as a part of the IP address change procedure. The MediaSense services may not function until the IP address change procedure is completed.

- Command privilege level: 1
- Allowed during upgrade: Yes

Command: **set network cluster secondary ip** *new_ip*

Details: *new_ip* is the new IP address for the secondary server

Example:

```
set network cluster secondary ip 9.9.9.9
Setting secondary ip to 9.9.9.9
Successful
```

set network ip eth0

This command sets the IP address for Ethernet interface 0. You cannot configure Ethernet interface 1.

The system asks whether you want to continue to execute this command.

Caution If you continue, this command causes the system to restart.

- Command privilege level: 1
- Allowed during upgrade: No

Caution This command may impact the synchronization of MediaSense services. Issue this command only as part of the IP address change procedure. The MediaSense services may not function until the IP address change procedure is completed.

Command: **set network ip eth0** *server new ip address mask gw*

Details:

- eth0 specifies Ethernet interface 0.
- *iserver new ip* specifies the new IP address that you want to assign.
- *address mask* specifies the IP mask that you want to assign.
- *gw* specifies the gateway

Example:

```
set network ip eth0 10.194.118.137 255.255.255.0 10.194.118.1

***   W A R N I N G   ***
You must first change the IP Address using the
<set network cluster server> CLI command BEFORE
changing it here or call recording will fail.
This will cause the system to restart.
=======================================================
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
=======================================================
Continue (y/n)? y
```

Show commands

The section provides details about the MediaSense-specific **show** commands.

show db_synchronization status

This command monitors the status of the **run db_synchronization** command. It displays one row for each database table and the corresponding status for that table.

Note In a multi-server deployment, you can only run this command on the secondary server.

Command: **show db_synchronization status** *database_name*

Details:

- *database_name* specifies the type of operation for the command to perform.

  The valid database names are:

  - *db_ora_config*
  - *db_ora_meta*

- For each database table, the output shows the start and end time of synchronization check, the number of rows to be checked, the number of rows already processed, and the replication check status.

  The replication check column displays the status of the replication as follows:

  - D = Defined
  - R = Running
  - C = Completed
  - F = Completed, but inconsistent
  - W = Pending Complete

Examples:

- `show db_synchronization status db_ora_config`
- `show db_synchronization status db_ora_meta`

show network cluster

This command displays the network information for all servers in the MediaSense cluster. This command provides details about the following information for each server: node ID, the IP address, the hostname, the server type (primary, secondary, or expansion), the server alias (if assigned), and authentication information.

Note To view all the details, this command requires the configuration service to be reachable and running on the primary or secondary server.

Command: **show network cluster**

Details: This command has no options.

Example:

```
show network cluster
1 10.10.10.92 mcs_vm92 Primary authenticated
2 10.10.10.93 mcs_vm93.cisco.com mcs_vm93 Secondary authenticated using TCP since Tue Aug
30 14:05:34 2011
3 10.10.10.100 mcs_vm100.cisco.com mcs_vm100 Expansion authenticated using TCP since Tue
Aug 30 14:05:24 2011
```

show tech call_control_service

This command displays information about the MediaSense call control service that runs on the system. The MediaSense call control service should be running for this command to execute successfully.

Command: **show tech call_control_service** *detailed*

Details:

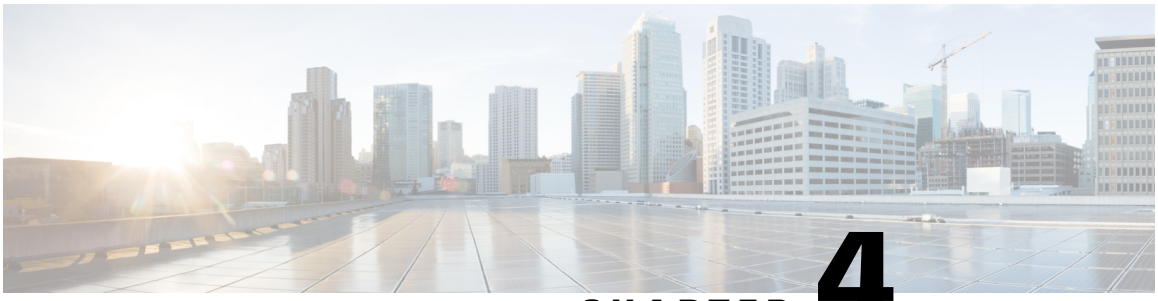
- When you issue this command, the MediaSense call control service details for this server are displayed in your CLI window.
- The *detailed* option specifies the type of information to download.

  If you do not specify this option, information is provided only about the system start time, system information, recording sessions information, state of each adapter, configuration information for each adapter, and statistics for each adapter.

  Specifying this option provides all thread details in addition to the system condition details specified above.

Examples:

- `show tech call_control_service`
- `show tech call_control_service detailed`

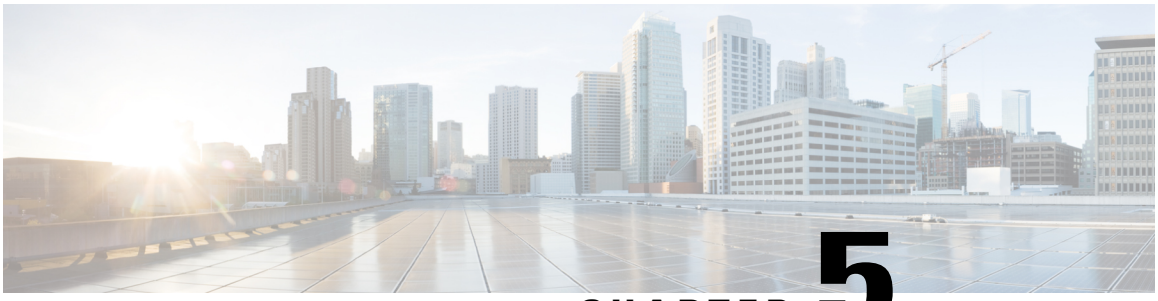


CHAPTER 4

Troubleshoot MediaSense

A Troubleshooting Tips for MediaSense wiki provides information to help resolve issues already reported by other users.

For help with troubleshooting the MediaSense APIs, see the "Before you start working with MediaSense APIs" and "Troubleshooting" sections in the *Cisco MediaSense Developer Guide*.



CHAPTER 5

MediaSense Terminology

This section identifies the commonly used MediaSense terms and provides a conceptual context for your reference and understanding.

- Play back, page 115
- Blog recording, page 116
- Media forking, page 116
- Sessions and recording sessions, page 116
- Glossary of Common Terms, page 117

Play back

You can search for a session and play the audio or video data for each session using the integrated Search and Play application or by using the MediaSense APIs. See the *Cisco MediaSense Developer Guide* (http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html) for more information about using the APIs.

You can play back MediaSense recordings using the Real Time Streaming Protocol (RTSP) or by downloading the recordings as .mp4 or .wav files.

- **Playback:** You can playback MediaSense recordings using the integrated Search and Play application or on any player which supports RTSP, .mp4, or .wav formats (for example, VLC—VideoLAN Client). If you listen to a forked media recording using VLC, you can only listen to one track at a time, and not both at the same time.
- **Download:** If you prefer to listen to both audio channels and view the video at the same time, export any MediaSense recording to .mp4 or.wav format using the **convertSession** API. This API returns the URL from which you can access the converted file. You can then download that file using standard HTTP access methods. Using a downloaded .mp4 or .wav file, you can listen to both audio channels and view the video at the same time.

  Converting to .mp4 or .wav format also makes the file portable and allows you to copy it to a location of your choice.
- Client applications can communicate directly with the MediaSense media service by using the `downloadUrl` parameter in the Session Query APIs. Each API has a `downloadUrl` only for AUDIO tracks.

You cannot download MediaSense video tracks in the RAW format. The downloaded recording is available only in the RAW format.

This URL is conditionally present in the session query response only if the `sessionState` is CLOSED_NORMAL or in the `sessionEvent` only if the eventAction is ENDED. For other sessions in other states, (ACTIVE, DELETED, or CLOSED_ERROR), `downloadUrl` is not available. See the *Playing Back Recordings* section in the *Cisco MediaSense Developer Guide* (http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html) for more information.

Blog recording

MediaSense enables you to create blog recordings (audio and video) using supported Cisco IP Phones. After the recordings are made, third-party applications can publish them.

A blog recording is initiated in one of the following ways:

- By a user who dials into a MediaSense server.
- By the MediaSense server calling a user phone in response to an API request.

Note CUBE deployments do not support direct outbound recording.

Media forking

All Cisco IP phones that MediaSense supports have a built-in bridge (BIB) that allows incoming and outgoing media streams to be forked. MediaSense makes use of this capability to record inbound and outbound forked media. For more details about media forking, see the Unified CM documentation at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

CUBE does not have a BIB because the call forking is performed within the CUBE application—not from a phone.

Sessions and recording sessions

In MediaSense, a *session* is a recorded monolog, dialog, or conference that can involve one or more participants. A MediaSense session is the same as a *recording session* in Unified CM. See the *Cisco Unified Communications Manager Features and Services Guide* at http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/prod_maintenance_guides_list.html for more information about recording sessions.

The participants in a session use a *device* to participate in a MediaSense session.

A *device* is a physical entity that can be an endpoint or a personal computer and refers to any item that can be recorded. A device is identified by a deviceRef which is a phone number or extension for each device. The deviceId is the unique identifier for each device and it corresponds directly to the name of the device (like the MAC address or Universal Device Identifier—UDI).

A session can be *live* (active) or *recorded* (completed). A live session can be monitored and recorded at the same time. A recorded session can be played back at any time.

Glossary

Active server

An active server is a primary server or secondary server with one instance of the API service, configuration service, call control service, media service, database service, and the SM agent. A MediaSense cluster must have one or two active servers. Replication is available in both active servers. To ensure high availability, if one active server goes down, the other active server can handle the complete load for both servers.

API service

The application programming interface (API) service is a feature service. Each MediaSense cluster can only have two instances of the API service. One instance is in the primary server and another instance is in the secondary server. Each API service must have a corresponding configuration service. If a MediaSense cluster has more than two servers, the additional servers do not have an API service or configuration service. Each instance of the API service corresponds directly to one instance of the meta database.

Call control

MediaSense uses the session initiation protocol (SIP) to control new calls, transferred calls, and calls that are placed on hold.

Call control service

Call control service communicates with the network layer, media service, and API service to provide key recording functions for MediaSense. One instance of the call control service is present in each server in a cluster.

Cluster

MediaSense servers are deployed in a cluster. A cluster can contain from one to five servers. Each cluster can provide basic media recording, database storage, and scalable recording capacity.

Configuration database

The configuration database is often referred to as the 'config' database. It stores log level and trace mask information. Each instance of the configuration database corresponds directly to one instance of the configuration service. Although the configuration database is not directly exposed to end users, you can indirectly configure functions such as service activation in the MediaSense Serviceability web portal.

Configuration service

Configuration service is a feature service. Each instance corresponds directly to one instance of the configuration database. Each MediaSense cluster can only have two instances of the configuration service. One instance is in the primary server and the other instance is in the secondary server. When one configuration service does not function, data can continue to be written to the other configuration service because MediaSense uses a peer-to-peer database model.

Each configuration service on the primary server and secondary server must have a corresponding instance of an API service. If a MediaSense cluster has more than two servers, the additional servers do not have a configuration service or an API service.

Database

MediaSense has two databases: the configuration database and the meta database. The general term "database" is used to refer to both of them.

Database service

The database service controls the configuration database and themeta database. Each MediaSense cluster can only have two instances of the database service. One instance is in the primary server and the other instance is in the secondary server.

Device

A *device* is a physical entity such as an end point or a personal computer that can be use to make recordings. Each device is identified by a unique deviceRef or Device Ref.

Device reference

A device reference is called a deviceRef in the API service and a device ref in the administration service. It refers to the phone number, IP address, or the URI/URL of each device. One or more participants can be associated with multiple device references.

Diagnostics

MediaSense diagnostics is a network service. This service is present in all MediaSense servers for debugging and troubleshooting purposes.

Expansion server

A MediaSense deployment can have a maximum of three expansion servers. Each expansion server has one instance of the call control service and one instance of the media Service. Expansion servers have no instances of the API service or the database service.

Feature service

Feature services enable you to configure and monitor all servers in a MediaSense cluster.

High availability

High availability means that if one server fails, the other server can handle the complete load for both servers in a MediaSense cluster. The data is load balanced between both servers and data replication is available in both servers.

Live (active) session

A live session is a call in progress and can be monitored and recorded at the same time. When it is finished, it becomes a recorded session that can be played back at any time.

Media service

Media service is a feature service. It terminates media streams for storage on a local disk. One instance of the media service is present in every server in a MediaSense cluster.

Media stream

A media stream refers to the packets going through an audio channel or video channel in a live or recorded session. It refers only to a live session. It does not refer to a recorded session. A recorded media stream is called a track.

Meta database

The meta database stores call history and metadata information associated with each recording. Each instance of the API service corresponds directly to one instance of the meta database.

Network services

Network services enable you to configure and monitor overall system functions. After you have installed MediaSense and re-booted your server, network services are enabled by default on all servers in a cluster.

Participant

A participant refers to people or end points involved in a session. Participants use a device to conduct a session. Participants are identified by a unique device reference, which is a phone number, IP address, or URL. During the same session, each track is associated with only one participant, the participant who is generating the media for that track. During different sessions, each track can have one or more participants.

Perfmon agent

This network service controls the performance monitoring infrastructure. It has no separate user interface and operates seamlessly within MediaSense serviceability administration.

Primary database

The configuration service in the first main server in any deployment is called the primary database. The configuration service in the second main server in any deployment is called the secondary database.

In a MediaSense cluster, configuration requests are sent to the primary database and the secondary database. If the primary database is functional, data is written to the primary database and then replicated to the secondary database. If the primary database is not functional, data is not written to ensure data integrity. If the primary database is not functional for a substantial period of time, you can manually promote the secondary database to be the new primary database so that data can be written to it. When the original primary database begins functioning again, it becomes the new secondary database.

Primary server

The primary server is the first server in the cluster. After you install MediaSense and re-boot the primary server, all MediaSense feature services are *enabled by default* .

Publisher

In MediaSense clusters, the primary and secondary servers are publishers (peer-to-peer).

Recorded (completed) session

A recorded session has been completed and can be played back at any time.

Recording types

MediaSense makes two types of recordings:

- Forked media recordings are made from IP phones. These recordings have two audio channels.

- Direct call recordings are made to and from MediaSense to any phone. These recordings have one audio channel and one optional video channel. (They are often called blog recordings in this document.)

Secondary database

The configuration database in the secondary server in a cluster is called the secondary database.

Secondary server

Each cluster can have only one secondary server. After you access the administration service and enable all feature services, you can assign that server as the secondary server. It is paired with a primary server to ensure high availability.

Session

A session is a recorded monologue call, dialog call, or conference call. A session is identified by a sessionID (or Session ID) and contains one or more tracks.

A MediaSense session has the same meaning as a recording session in Unified CM. See the *Cisco Unified Communications Manager Features and Services Guide* (http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/prod_maintenance_guides_list.html) for more information about its recording sessions.

Session ID

The unique identifier for a session.

SM agent

Storage management agent (SM agent) monitors the overall storage in each server in a cluster and generates threshold events based on disk usage. It is available in all servers in the cluster.

System service

This network service controls service operations. It does not have a separate user interface and operates seamlessly within the MediaSense administration service and MediaSense serviceability administration.

Tag

System-defined tags are brief, arbitrary text strings that associate individual sessions using the Web 2.0 APIs. MediaSense stores tags with each session. MediaSense uses tags to mark certain actions which occurred during the session (such as , pause and resume) or to mark when the media inactivity state changes (as reported by the SIP signaling). While most tags are associated only with a session, media inactivity state change tags are associated with a session and with a specific track in the session.

Track

A track identifies each media stream and quantifies it with additional data such as participants, duration, startDate, and trackNumber. Each track is specific to one audio stream or one video stream. Each track can be associated with multiple device references. Each session contains one or more tracks.

Track ID

The unique identifier for a track.