Cisco MediaSense User Guide, Release 11.5(1)

First Published: 2016-08-10
Last Modified: 2018-06-06

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.
# CONTENTS

## PREFACE
Preface  xi  
Change History  xi  
Related Documentation  xiv  
Obtaining Documentation and Submitting a Service Request  xiv  
Field Alerts and Field Notices  xiv  
Troubleshooting  xiv  
Documentation Feedback  xiv  
Documentation Conventions  xv

## CHAPTER 1
MediaSense Overview  1  
About MediaSense  1  
Architecture  1  
Services  2  
Network Services  2  
Feature Services  3  
MediaSense Deployments - Types of Recordings  3  
Cisco Unified Communications Manager Network-Based Recording  4  
Unified Communications Manager Deployments  4  
Cisco Unified Border Element Deployments  4  
Cisco Unified Communications Manager and Cisco Unified Border Element Scenario Differences  6  
MediaSense Deployments - Streaming Service  7  
Unified CVP Deployments  7  
MediaSense Deployments - Cluster Options  8  
Single-Server Deployments  9  
Dual-Server Deployments  10  
Three-Server Deployments  11
Hardware Requirements 38
Software Requirements 38
License Requirements 38
Other Requirements 39
Installation 39
Install MediaSense and Unified OS 39
Initial Configuration 43
Complete Setup for Primary Server 43
Details for Secondary and Expansion Servers 46
Finish Setup for Subsequent Servers 46
Confirming MediaSense Operation 48
Upgrade MediaSense 49
Upgrade Considerations 50
Virtual Machine Parameters Settings for Refresh Upgrade 51
Upgrade Cluster to Release 11.x(x) 52
Node Upgrade Procedures 53
Upgrade Nodes From a Local Source 53
Remote Sources 54
Rollback Cluster 57
Install COP Files 57
Language Pack 58

CHAPTER 3

Advanced Tasks 59
Unified Communications Manager Provisioning for MediaSense 59
Setup Call Control Service Connection 59
MediaSense Setup with Cisco Unified Border Element 61
Manage Unified Communications Manager Users 61
Cisco MediaSense Provisioning for Unified Border Element 62
Unified Border Element and MediaSense Setup 62
Unified Border Element Gateway Accessibility 63
Unified Border Element View Configuration Commands 63
Global-Level Interoperability and MediaSense Setup 64
Set Up Global Level 64
Dial-Peer Level Setup 65
CHAPTER 5

Cisco MediaSense Serviceability 117

MediaSense Serviceability 117
Access MediaSense Serviceability 118
Trace Configuration 118
Trace Log Levels 119
Contents

CHAPTER 6

MediaSense Command Line Interface 141

Introduction 141

CLI Access 141

Trace Flags 120
Trace File Location 121
Setup Trace File Information 121
Trace File Interpretation 122
Performance Logging 122
Dump Trace Parameters 123
Serviceability Tools 123
  Control Center Network Services 123
  Manage Network Services 124
  Control Center Feature Services 124
  Manage Feature Services 124
  Media Service Call Control Service or Database Service Reactivation 125
Unified RTMT Administration 125
  Unified RTMT Installation and Setup 126
    Download the Unified RTMT Plug-In 126
  Unified RTMT Upgrade 126
  Unified RTMT Multiple Copy Installations 127
Server Status Monitoring 127
  Performance Monitoring Counters 127
    Unified RTMT for Performance Monitoring 127
  System Condition and Perfmon Counter Alerts 127
    AMC Service and Unified Communications Manager Setup 131
Trace and Log Central Unified RTMT Setup 131
  File Collection 132
    Crash Dump Collection 132
    Remote Browse Folder Names and Services 132
    Perfmon Agent and Counters 133
Cisco Prime Collaboration Assurance Administration 138
Access Serviceability User Interface for Other Servers in Cluster 139
Other Browser-Based Serviceability Tools 140
Preface

- Change History, on page xi
- Related Documentation, on page xiv
- Obtaining Documentation and Submitting a Service Request, on page xiv
- Field Alerts and Field Notices, on page xiv
- Troubleshooting, on page xiv
- Documentation Feedback, on page xiv
- Documentation Conventions, on page xv

Change History

This table lists and links to changes made to this guide. Earliest changes appear in the bottom rows.
<table>
<thead>
<tr>
<th>Change</th>
<th>See</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added the section Virtual Machine Parameters Settings for Refresh Upgrade</td>
<td>Virtual Machine Parameters Settings for Refresh Upgrade, on page 51</td>
<td></td>
</tr>
<tr>
<td>Added the section IPv6 Support</td>
<td>IPv6 Support, on page 30</td>
<td></td>
</tr>
<tr>
<td>Added the section Finesse Role-Based Access</td>
<td>Finesse Role-Based Access, on page 25</td>
<td></td>
</tr>
<tr>
<td>Added the section Secured Communication</td>
<td>Secured Communication, on page 26</td>
<td></td>
</tr>
<tr>
<td>Added the section Single Sign-On</td>
<td>Single Sign-On, on page 25</td>
<td></td>
</tr>
<tr>
<td>Added the section Change IPv6 Address of Primary Server</td>
<td>Change IPv6 Address of Primary Server, on page 74</td>
<td></td>
</tr>
<tr>
<td>Added the section Change IPv6 Address of Secondary Server</td>
<td>Change IPv6 Address of Secondary Server, on page 77</td>
<td></td>
</tr>
<tr>
<td>Added the section Change IPv6 Address of Expansion Server</td>
<td>Change IPv6 Address of Expansion Server, on page 79</td>
<td></td>
</tr>
<tr>
<td>Added the section Playlist Manager</td>
<td>Playlist Manager, on page 106</td>
<td></td>
</tr>
<tr>
<td>Added the section Upload Cisco Finesse Certificate to Cisco MediaSense Server</td>
<td>Upload Cisco Finesse Certificate to Cisco MediaSense Server, on page 94</td>
<td></td>
</tr>
<tr>
<td>Added the section Unified CVP Deployments</td>
<td>Unified CVP Deployments, on page 7</td>
<td></td>
</tr>
<tr>
<td>Added the section Setup Call Control Service Connection</td>
<td>Setup Call Control Service Connection, on page 59</td>
<td></td>
</tr>
<tr>
<td>Updated the section Search For, Play, or Download a Recorded Call</td>
<td>Search For, Play, or Download a Recorded Call, on page 17</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>See</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Initial Release of Document for Release 11.0(1)</td>
<td></td>
<td>July 2015</td>
</tr>
<tr>
<td>Updated the <em>Search and Play Configuration</em> section</td>
<td><em>Search and Play Configuration</em>, on page 111</td>
<td></td>
</tr>
<tr>
<td>Updated the <em>Archival</em> section</td>
<td><em>Archival</em>, on page 108</td>
<td></td>
</tr>
<tr>
<td>Added the section <em>Search for an Archive Call</em></td>
<td><em>Search for Archived Calls</em>, on page 20</td>
<td></td>
</tr>
<tr>
<td>Added the section <em>Session Errors in MediaSense Search and Play</em></td>
<td><em>Session Errors in MediaSense Search and Play</em>, on page 22</td>
<td></td>
</tr>
<tr>
<td>Added the section <em>Cisco Prime Collaboration Assurance Administration</em></td>
<td><em>Cisco Prime Collaboration Assurance Administration</em>, on page 138</td>
<td></td>
</tr>
<tr>
<td>Added <em>Agent Data Information</em> in the Search for, Play, and Download a Recorded Call section</td>
<td><em>Search For, Play, or Download a Recorded Call</em>, on page 17</td>
<td></td>
</tr>
<tr>
<td>Added new counters in the Class: MediaSense API Service <em>Perfmon Agent and Counters</em> section</td>
<td><em>Perfmon Agent and Counters</em>, on page 133</td>
<td></td>
</tr>
<tr>
<td>Initial Release of Document for Release 10.5_SU1</td>
<td></td>
<td>October 2014</td>
</tr>
<tr>
<td>Added the section <em>In-Browser Playback</em></td>
<td><em>In-Browser Playback</em>, on page 21</td>
<td></td>
</tr>
<tr>
<td>Added the section <em>Finesse AgentInfo Gadget</em></td>
<td><em>Finesse AgentInfo Gadget</em>, on page 23</td>
<td></td>
</tr>
<tr>
<td>Added the section <em>Search and Play Configuration</em></td>
<td><em>Search and Play Configuration</em>, on page 111</td>
<td></td>
</tr>
<tr>
<td>Added the section <em>Unified Communications Manager Network-based Recording</em></td>
<td><em>Cisco Unified Communications Manager Network-Based Recording</em>, on page 4</td>
<td></td>
</tr>
<tr>
<td>Added the section <em>Archival</em></td>
<td><em>Archival</em>, on page 108</td>
<td></td>
</tr>
<tr>
<td>Added the section <em>Other Browser-based Serviceability Tools</em></td>
<td><em>Other Browser-Based Serviceability Tools</em>, on page 140</td>
<td></td>
</tr>
</tbody>
</table>
Related Documentation

<table>
<thead>
<tr>
<th>Document or Resource</th>
<th>Link</th>
</tr>
</thead>
</table>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the RSS feeds. These services are a free service.

Field Alerts and Field Notices

Note that Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Field Alert and Cisco Field Notice notifications. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.


Troubleshooting

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*.

Documentation Feedback

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

ccebu_docfeedback@cisco.com

We appreciate your comments.
# Documentation Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **boldface** font | Boldface font is used to indicate commands, command names, and keywords, such as user entries, keys, buttons, and folder and submenu names. For example:  
  • Choose **Edit > Find**.  
  • Click **Finish**. |
| **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. |
MediaSense Overview

About MediaSense

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 Cisco Unified Border Element 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 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.

Related Topics

Authentication, on page 25

Architecture

MediaSense is part of the Unified Communications solution and runs on Cisco Unified Operating System, Release 11.5.

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 Communications Manager) for audio recording.
  • Integration with Cisco Unified Border Element (Unified Border Element) for audio and video recording.

## Services

### Network Services

You can use the following network services with MediaSense:

- **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 Communications Manager 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 Communications Manager user interface and Unified Communications Manager 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.

**MediaSense Deployments - Types of Recordings**

Based on recordings, there are three types of MediaSense deployments.

- Cisco Unified Communications Manager Network-Based Recording
- Cisco Unified Communications Manager Deployments
- Cisco Unified Border Element Deployments

**Related Topics**

- Cisco Unified Communications Manager Network-Based Recording, on page 4
- Unified Communications Manager Deployments, on page 4
- Cisco Unified Border Element Deployments, on page 4
Cisco Unified Communications Manager Network-Based Recording

With Unified Communications Manager network-based recording (NBR), you can use a gateway to record calls. NBR allows the Unified Communications Manager to route recording calls, regardless of device, location, or geography.

With NBR, call recording media can be sourced from either the IP phone or from a gateway that is connected to the Unified Communications Manager over a SIP trunk. Unified Communications Manager dynamically selects the right media source based on the call flow and call participants.

NBR offers an automatic fallback to Built-in-Bridge (BiB) when the Integrated Services Routers (ISR) are unavailable because no separate recording configuration is required. This fallback is useful in cases where customers want to include agent-agent consult calls in the recording policies because Unified Border Element cannot record consult calls, so BiB needs to be enabled separately.

For more information on Unified Communications Manager NBR, refer to Cisco Collaboration System Solution Reference Network Designs.

Call Correlation

Both NBR and BiB calls can be correlated using xRefci, which is available from Unified Communications Manager JTAPI. CISCO-GUID is not required, which means that neither the CTI server nor CTIOS connections are required. Because there is a single correlation identifier, correlation across components is stronger and can be done in a uniform way independent of the call flow. Using NBR, directly-dialed as well as dialer-initiated outbound calls can be correlated with their appearance in other solution components. Using NBR, TDM gateway recording is automatically used without splitting the capacity of the router.

---

**Note**

MediaSense supports TDM gateway recording.

---

Unified Communications Manager Deployments

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

A basic Unified Communications Manager 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 Design Guide 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 Communications Manager documentation.

---

Cisco Unified Border Element Deployments

Cisco Unified Border Element 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 Unified Border Element to enable recording without regard to the endpoint type. Because of this capability, MediaSense can use Unified Border Element to record inbound and outbound media.

For more information about Cisco Unified Border Element, see the Unified Border Element documentation.

The following figure illustrates a MediaSense deployment with Cisco Unified Border Element. Even in a Cisco Unified Border Element deployment, MediaSense depends on Unified Communications Manager to provide authentication services.

*Figure 1: MediaSense Deployment with Cisco Unified Border Element*

In the preceding illustration, the Real-Time Protocol (RTP) carries voice data between the endpoints and Cisco Unified Border Element. The Session Initiation Protocol (SIP) carries call signaling information between the endpoints and Unified Border Element. Two RTP unidirectional streams represent two audio streams forked from Cisco Unified Border Element to MediaSense. Streams from Cisco Unified Border Element to MediaSense are unidirectional because only Cisco Unified Border Element sends data to MediaSense; MediaSense does not send any media to Cisco Unified Border Element. Cisco Unified Border Element has three dial-peers: inbound, outbound, and forking.

Typically, Cisco Unified Border Element 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 Cisco IOS version. (For more information, see the Cisco Unified Border Element documentation.)

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 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
feature cuts the router capacity in half and Cisco Unified Border Element 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 and the MediaSense FAQ page on How to Configure a TDM Gateway for Media Forking?

Related Topics
Dial-Peer Level Setup, on page 65

### Cisco Unified Communications Manager and Cisco Unified Border Element Scenario Differences

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

**Note**
See the Cisco MediaSense Design Guide for further details about Unified Border Element media forking and UC endpoints media forking.

Regardless of whether MediaSense is deployed with Unified Communications Manager or Unified Border Element, the 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.

#### Table 1: Unified Communications Manager and Unified Border Element Scenario Differences

<table>
<thead>
<tr>
<th>MediaSense Feature</th>
<th>With Unified Communications Manager (Built-in-Bridge or Network-based Recording)</th>
<th>With Unified Border Element Dial Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiating recordings</td>
<td>The direct outbound recording scenario, which is initiated when a client calls the startRecording API, is supported with Unified Communications Manager deployments.</td>
<td>The direct outbound recording scenario, which is initiated when a client calls the startRecording API, is not supported with Unified Border Element deployments.</td>
</tr>
<tr>
<td>Recording</td>
<td>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).</td>
<td>Recording uses SIP devices (referred to as SIP User Agent in Unified Border Element). As long as the call is processed by Unified Border Element 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.</td>
</tr>
<tr>
<td>MediaSense Feature</td>
<td>With Unified Communications Manager (Built-in-Bridge or Network-based Recording)</td>
<td>With Unified Border Element Dial Peer</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Identifying tracks for calling versus called party</td>
<td>The numerically smaller xRefCi parameter usually refers to the track of the calling party.</td>
<td>Track 0 contains the media stream corresponding to the dial-peer in which the media recording profile is configured.</td>
</tr>
<tr>
<td>See the FAQs for MediaSense website (How do you determine which track has the calling and which has the called party?)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recording session</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>See the Cisco MediaSense Developer Guide for details about recording sessions and hold/resume, pause/resume, transfer/conference commands.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Differences in the captured recording data</td>
<td>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 Administration Guide.</td>
<td>Unified Border Element 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.</td>
</tr>
<tr>
<td>See the Cisco MediaSense Design Guide.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mid-call codec change</td>
<td>Does not generate mid-call codec changes.</td>
<td>A new session starts.</td>
</tr>
<tr>
<td>Endpoint MAC address</td>
<td>Captured.</td>
<td>Not captured.</td>
</tr>
<tr>
<td>Recording media source</td>
<td>The endpoints provides the forked media.</td>
<td>Unified Border Element provides the forked media.</td>
</tr>
</tbody>
</table>

**MediaSense Deployments - Streaming Service**

**Unified CVP Deployments**

MediaSense offers two kinds of RTP (Real-time Transport Protocol) playback:

- RTSP (Real Time Streaming Protocol) playback of recordings
- SIP playback of uploaded media files

When MediaSense is used as the RTSP streaming server, it combines both the kinds of playback to provide RTSP playback of audio component of upload media files. As a media server, MediaSense allows creation, management and playback of playlists composed of uploaded media files.
For example:

In a Unified CVP deployment, MediaSense acts as a media server.

Following figure shows a Unified CVP deployment where a MediaSense server is used for streaming pre-recorded media to the gateway over RTP.

Figure 2: MediaSense Server in a Unified CVP deployment

Related Topics

Uploaded Media Files, on page 32

MediaSense Deployments - Cluster Options

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 area networks (WAN) are not supported. All MediaSense servers and Unified Communications Manager 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 milliseconds.

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:
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 fewer 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).

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`.

Related Topics

Install MediaSense and Unified OS, on page 39

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 3: Cisco MediaSense Single-Server Deployment

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. For more information on deployment models, refer to the Cisco MediaSense Design Guide.

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
• Storage Management agent (SM agent)

Figure 4: Dual-Server Deployment

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.
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.

Note

See the Cisco MediaSense 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

Figure 5: Three-Server Deployment

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.
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 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

**Figure 6: Five-Server Deployment**

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.

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 Communications Manager cannot contact one of the MediaSense servers, you must ensure that an alternate server is available for Unified Communications Manager or Unified Border Element to make the required connection.

For more information, see the Cisco MediaSense Design Guide.

**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.

---

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.

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. Data written to the primary server is also replicated to the secondary server, and vice versa.

The replication operation 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 Design Guide.

**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 percent 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 metadata 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:

```bash
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.

<table>
<thead>
<tr>
<th>MediaSense Scenarios</th>
<th>With Unified Communications Manager (Built-in-Bridge or Network-based Recording)</th>
<th>With Unified Border Element Dial Peer Recording</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal scenario</td>
<td>The Unified Communications Manager 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.</td>
<td>Unified Border Element always sends a call to the first MediaSense server in the media-recording list.</td>
</tr>
<tr>
<td>Failed server scenario</td>
<td>Unified Communications Manager uses the next available MediaSense server in the list.</td>
<td>Unified Border Element uses the next available MediaSense server in the media-recording list.</td>
</tr>
</tbody>
</table>

## Failure Condition Considerations

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

*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:

- Volume of data written to the surviving server when one server is down
- Duplex network connection speed between the two servers
- 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 percent full.** If the failed server is brought back before ora_ersb is 90 percent full on the surviving server, no metadata is lost.
- **When ora_ersb is more than 90 percent full.** If the ora_ersb becomes 90 percent 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 reestablished 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 in 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 Design Guide.
MediaSense Features

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. You can search and play back archived as well as nonarchived recordings in the MediaSense Search and Play application.

The Archive Calls tab displays in MediaSense Search and Play when the Enable Search on Archived Recordings check box is checked in the MediaSense Archive Configuration screen.

To access the Search and Play application, do one of the following:

- Open the link, https://<hostname>:8440/mediasense, in a browser.
- Click the Cisco MediaSense Search and Play link from the main MediaSense access window at http://<MediaSense hostname>.

Before launching Search and Play, install the 32-bit version of JDK on a 32-bit Windows machine, the 64-bit version of JDK on 64-bit Windows machine, and the 64-bit version on Mac computers. 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, make sure to accept a popup security warning every time the Java application is executed; meaning that you must accept a security warning every time a recording is played.

Because 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 your 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 (Search and Play application users encounter security warning before each playback).

The media player takes longer to start in Windows Internet Explorer than in Mozilla Firefox. In Internet Explorer, you may also see an option to open a downloaded jnlp file.

When prompted for sign-in credentials, use the API user credentials defined on the MediaSense API User Configuration page of the Administration application.
You are logged out from the MediaSense Search and Play application if the session remains idle for 30 minutes. MediaSense Search and Play AXL user credentials are stored in the MediaSense server cache, which is updated every 30 minutes. In case the AXL user credentials are revoked in MediaSense Administration and you are logged out of MediaSense Search and Play, you cannot sign in to MediaSense Search and Play with the existing user credentials once the cache is updated.

Search For, Play, or Download a Recorded Call

There are multiple ways to search for the 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, Active Calls, or Archive Calls searches by clicking these tabs at any time.

Step 2 For a simple search, enter either a participant identifier or a tag in the search box and click Search.

- For participant ID, enter the complete value of the identifier. To search for multiple participants, use a space to separate each entry; the delimiter is considered as an OR operator.

- For tags, you can enter one or two letters because a complete value is not required. For more information, refer to Tags in Advanced Search (Step 3).

Use a space to separate each entry; the delimiter is considered as an OR operator. By default, the simple search returns calls within the last 7 days.

Step 3 For an advanced search, enter values in any of the search parameters from the Search Recordings drop-down menu.

Note Enter a value in not more than one of the following fields: Participant, Login Name, Login Id, First Name, Last Name, Line Name, or xRefCi. In case you enter a value in more than one of these fields, it usually returns no search results.

The search parameters include:

- **Session ID**— The identifier of a recording session with one or more tracks associated with it. Enter a session identifier in the text box. Every recording has a unique sessionId. So, when you search a recording with a sessionId, other entered search parameters are passed over. Only one Session ID can be searched at a time.

- **Participant(s)**— The identifier for recording session participants, which is a 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 the participants (the delimiter is treated as an AND operator).

- **Agent(s)**— Enter the following details:

  - **Login Id(s)**— The login identifier of the agent associated with a recording session in one or more tracks. Enter an agent login identifier in the text box. Multiple agent login identifiers can be searched by separating the identifiers with a comma or a space. When multiple participants are defined, the
search returns only those calls containing all the agent login ids (the delimiter is treated as an AND operator).

- **Login Name(s)**— The login name of the agent associated with a recording session in one or more tracks. Enter an agent login name in the text box. Multiple agent login names can be searched by separating the identifiers with a comma or a space. When multiple participants are defined, the search returns only those calls containing all the agent login names (the delimiter is treated as an AND operator).

- **First Name**— The first name of the agent associated with a recording session in one or more tracks. Enter an agent first name in the text box.

- **Last Name**— The last name of the agent associated with a recording session in one or more tracks. Enter an agent last name in the text box.

- **Line Name**— The line name appears on a phone as the calling party if configured in Unified Communications Manager. Enter a line name in the text box. Only one line name can be searched at a time, though several related calls are returned if they contain that line display name value.

- **Tag**— 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.

- **XRefCI**— The recording session identifier that is associated with the recordings that are controlled by Unified Communications Manager. Most of these recording types have at least two such identifiers. Enter a recording session identifier in the text box. Only one XRefCI can be searched at a time, though several related calls are returned if they contain that xRefCI value.

- **CCID**— The recording session identifier that is associated with the recordings that are controlled by Unified Border Element. 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. You can also select the time zone from the Zone drop-down list.

  **Note** 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 impacts 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**.

A list of recordings appears based on the specified search criteria. The list shows one of the following, based on the order of priority as shown:

- Line name
- First name and Last name combination
- First name or Last name, whichever exists
• Extension number

The list also shows duration, date, time, and time zone of the recordings.

**Step 5**

Click the + icon corresponding to a recording to view the details.

The details include session ID, extension, Login ID, Last Name, First Name, Login Name, Line Name, XRefci, CCID, Codec, and Time.

Click the following icons to perform respective action.

• **Expand Call** icon—To view the strongly associated recording sessions displayed in the Associated Session box. Strongly associated sessions have at least one common xRefCi value (in case of sessions recorded through Unified Communications Manager), and at least one common CCID value (in case of sessions recorded through Unified Border Element). Each session in the displayed list can be individually played or downloaded.

  **Note** MediaSense supports call association for sessions generated through the following modes.

  • Unified Communications Manager Built-in-Bridge (BiB) forking

  • Unified Communications Manager Network-based Recordings (NBR)

  • Unified Border Element Dial Peer

• **Delete** icon—To delete a recording.

  On clicking the icon, the following message appears.

  Are you sure you want to delete this recording?

  Click OK.

  The recording gets deleted and the following message appears.

  Session deleted successfully.

  **Note** The Delete icon is enabled if the Enable Delete Functionality check box is checked in the MediaSense Search Play Configuration window of MediaSense Administration.

• **Download** icon—To download a recording.

  You can download a recording in the .wav or .mp4 format.

• **Play** icon—To play back a recording.

**Step 6**

To sort the files by age or duration, click the **Sort by** drop-down menu.

**Note** To select the number of results displayed on each page and to step through the result pages, use the Previous and Next buttons.

**Related Topics**

Search and Play Configuration, on page 111
Search for Archived Calls

To search archive calls, you must enter either a session ID or a participant ID along with the date range, otherwise the following message appears.

Archive searches require a Session ID or a Participant value to search on. Please enter a Session ID or a Participant ID.

Perform the following steps:

Procedure

**Step 1** Enter the unique session identifier of the recording session you want to search in the **Session ID** text box.

**Step 2** Enter the participant identifier (phone extension) of the recording session you want to search in the **Participant** 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 the participants (the delimiter is treated as an AND operator).

**Step 3** Select the date range 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.

**Note** 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 impacts system performance.

**Step 4** Click **Search**.

A list of archived calls within the specified criteria appears.

Related Topics

Archival, on page 108

Playback a Recording

To playback a recording, Mediasense Search and Play offers two players:

- Inbuilt Media Player
- Inbrowser Player

Media Player

MediaSense has an inbuilt media player in the Search and Play application to play a recording. To run the media player, you should have the updated Java version (For Java version, refer the Web Browsers section in the Cisco MediaSense Design Guide). The track slider displays the progress of the audio recordings. The slider can be dragged to right to forward or left to rewind the recording being played.

When a recording finishes, and you want to replay it, drag the slider back to the starting point, however, it should be done in less than 30 seconds. After 30 seconds, the playback session ends and the player get closed.

**Note** For video recordings, the track slider is not supported. However, the timer is displayed to view the progress of the video recordings.
You can increase/decrease the volume by dragging the slider on the Volume bar.

Limitations of the media player:

- Time is not displayed while you drag the slider for rewind or forward.
- Pause button does not automatically convert to the Play button after a recording ends.
- Media Player session gets aborted if the Play and Pause button is clicked more than twice after the slider reached the end of the playback stream.
- During a playback session, when you click any point to rewind/forward, the track slider moves nearby the clicked point but not the exact point.

**Note**

The duration of a recording displayed on the media player differs from the duration shown in the Search and Play application for the same recorded session. However, the playback always includes the complete recording. The difference in the duration is because the media player shows the duration of media that was actually received, whereas the Search and Play application shows the call duration from the perspective of SIP signaling.

When exiting the media player, users may receive a warning stating "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.

**In-Browser Playback**

MediaSense has an in-browser playback that uses the HTML5 playback feature of the browser to play back a recording. The in-browser player converts a recording into mp4 format irrespective of its original format. It has play, pause, and volume controls and displays the progress of the recording being played. The in-browser playback does not require you to download the recording or manage security certificate issues, which is an advantage over the built-in Java media player. By default, MediaSense uses the Java media player for playback.

To enable in-browser playback, you need to configure the settings in the Search and Play Configuration window (Cisco MediaSense Administration > Administration > Search and Play Configuration). Currently, in-browser playback is supported for stored audio calls only. The video recordings are played back on Java media player only irrespective of the configurations being saved in the Search and Play Configuration window.

MediaSense servers offer self-signed certificates that are initially not included in the browser's trusted authority. So to run the in-browser player, this self-signed certificate must be added to the trusted root authority of the browser. For details on how to add a self-signed certificate in a browser, refer How to configure a browser to run in-browser player in MediaSense?

If you are using CA signed certificates, then the CA certificate must be added to the trusted root authority of the browser.

**Note**

To run the in-browser player, set the server configuration as:

1. Make sure MediaSense nodes are added to the cluster with the respective FQDN in the MediaSense Configuration window of Cisco MediaSense Administration.

2. In the Administrator CLI of all the nodes of MediaSense cluster, enter the following command to configure all media URLs to contain FQDN.

   ```
   set useHostNameForMediaURL true
   ```
Session Errors in MediaSense Search and Play

For the sessions that are in the CLOSED_ERROR state, the MediaSense Search and Play application displays one of the following errors.

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orphaned Session</td>
<td>The session was orphaned. This can occur if (for example) the session was forcibly closed after service restart.</td>
</tr>
<tr>
<td>MEDIA_FORMAT_ERROR</td>
<td>The uploaded video file is not processed because of an incompatible codec, or container.</td>
</tr>
<tr>
<td>Record Response Fail</td>
<td>The Call Control server receives an error response from the Media (recording) server for an open-session or close-session request.</td>
</tr>
<tr>
<td>Record Response Timeout</td>
<td>The Call Control server is timed out waiting for response from the Media (recording) server for an open-session or close-session request.</td>
</tr>
<tr>
<td>SIP Signal Error</td>
<td>The Call Control server detects a SIP signaling error. For example, a missing ACK.</td>
</tr>
<tr>
<td>SIP Signal Error</td>
<td>The recording was canceled by the Call Control server, such as CANCEL or premature BYE.</td>
</tr>
<tr>
<td>Unsupported Codec</td>
<td>The codec is not supported.</td>
</tr>
<tr>
<td>Zero Size Tracks</td>
<td>The session was closed successfully, however, all tracks have size as zero.</td>
</tr>
</tbody>
</table>

Finesse Gadgets

Before you deploy the MediaSense gadget on Finesse desktop layout, please refer to the Cisco Finesse Configuration for various settings that is required to deploy the gadgets.

Search and Play Gadget

Search and Play gadget is a web interface available on the Finesse desktop to access all the recordings stored in MediaSense. Using the Search and Play gadget, Finesse supervisors and agents can search, download, and playback recordings.

Configuration of Search and Play Gadget on Finesse Desktop

To configure Search and Play gadget on Finesse desktop, perform the following steps:

Procedure

**Step 1**
Log in to Cisco Finesse Administration with valid credentials.

The Cisco Finesse Administration screen appears.
Step 2
Click the Desktop Layout tab.
The Manage Desktop Layout screen appears.

Step 3
In the Finesse Layout XML section, add the gadget tag within the layout xml.
The gadget tag has the xml path of the gadget.
For example: <gadget>https://<Host>:<Port>/ora/gadget/MediaSenseGadget.xml</gadget>

---

Search and Play Gadget Setup in Finesse Desktop

To access Search and Play gadget for the first time through Finesse desktop, perform the following steps:

Procedure

Step 1
Login to Finesse Desktop.

Step 2
In the Recordings section, click the Add Certificate button.
A pop-up window appears stating that the connection is untrusted.

Step 3
To add the trusted certificate, click the Add Exception button.
The certificate is added successfully and the Finesse Desktop appears displaying the recordings.

---

Finesse AgentInfo Gadget

Finesse AgentInfo gadget conveys agent information from Finesse to MediaSense, which includes login ID, team ID, login name, team name, first name, and last name. The information is linked with all the calls in which the agent is involved. In MediaSense, the agent information is retrieved from getSessions API. The gadget is deployed on the Finesse Agent desktop and can be hosted on both primary and secondary MediaSense nodes, however, not simultaneously.

When an agent signs in to the Finesse desktop with valid Finesse credentials, the gadget signs in to the MediaSense server.

Note
In case of gadget sign-in failures, the gadget retries every three minutes indefinitely. Sign-in is reattempted for all the failure cases except for the sign-in with invalid credentials.

The gadget is present on the agent's desktop as a title and a frame. However, it performs a number of functions that are invisible to the agent.

As a result of these actions, MediaSense knows about the agents' details and their login extensions as well as keeping track of the time the agent signs in and out. This also helps MediaSense to keep its data accurate, even in case of a browser failure.

Related Topics
Configuration of AgentInfo Gadget on Finesse Desktop, on page 24
Configuration of AgentInfo Gadget on Finesse Desktop

To deploy AgentInfo gadget on Finesse desktop, perform the following tasks:

**Procedure**

**Step 1**  
Log in to Cisco Finesse Administration with valid credentials.  
The Cisco Finesse Administration screen appears.

**Step 2**  
To configure the global Finesse layout, click the **Desktop Layout** tab to bring up the **Manage Desktop Layout** screen.  
To configure the Finesse layout on a team-by-team basis, click the **Team Resources** tab and select the team whose layout you would like to edit. In the team **Desktop Layout** sub-tab, ensure the "Override System Default" checkbox is checked, and proceed to edit the layout.

**Step 3**  
In the **Finesse Layout XML** section, add the gadget tag within the agent layout. It should preferably be in the page tag.  
For example:

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
    <gadget>https://<MS_FQDN>:8440/ora/gadget_agentInfo/MSAgentInfoGadget.xml</gadget>
    <!-- Other gadgets may be contained here-->
  </page>
</layout>
```

**Step 4**  
Add the same gadget in the supervisor role. It should preferably be in the page tag.  
For example:

```
<layout>
  <role>Supervisor</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
    <gadget>https://<MS_FQDN>:8440/ora/gadget_agentInfo/MSAgentInfoGadget.xml</gadget>
    <!-- Other gadgets may be contained here-->
  </page>
</layout>
```

**Note**  
The AgentInfo gadget does not render anything inside the page tag. The gadget runs silently in the background.  
If you want to see the MediaSense Search and Play gadget for agents as well, then add the same gadget in Agent role in a similar way.

**Step 5**  
Save the **Finesse desktop layout**.

**Note**  
The gadget can be hosted on both primary and secondary MediaSense nodes, however, not simultaneously.  
For Finesse AgentInfo gadget to function efficiently in Internet Explorer 11, set the Document Mode as Edge (default) in Internet Explorer tools. For more information, refer **Internet Explorer requirements to run Finesse AgentInfo gadget**.
Security

Authentication

Authentication is a process to identify a user. MediaSense does not authenticate user credentials by itself. It uses third party for authentication. In Mediasense, authentication can be done in two ways.

- AXL Authentication
- Finesse Authentication

Related Topics

About MediaSense, on page 1

AXL Authentication

MediaSense uses AXL (Administrative XML Layer) to authenticate a user. AXL is an Application Programming Interface (API) to insert, retrieve, update, and remove data from a database using an eXtensible Markup Language (XML) Simple Object Access Protocol interface. MediaSense authenticates a user through Cisco Unified Communications Manager AXL.

Finesse Authentication

MediaSense uses Finesseserver as one of the authentication servers (Proxy authentication) to authenticate user credentials. The user credentials used for login to Finessedesktop can also be used to login to the MediaSense Search and Play application. In Finesses, the background scripts fetch the user credentials and automatically log in to AgentInfo gadget and Search and Play gadget. Once the Finesse Agent desktop is logged in, Mediasense Search and Play and AgentInfo gadgets are uploaded (in case gadgets are configured). Both gadgets invoke signIn API towards MediaSense to establish individual API sessions.

Single Sign-On

MediaSense supports deployment of Search and Play and AgentInfo gadgets in single sign-on based Finesse deployments. Single sign-on is an authentication process that allows a user to enter one username and password and access all the components of the Contact Center Solution without signing on again. Single sign-on uses SAML authentication protocol to authenticate the user.

Authorization

Finesse Role-Based Access

MediaSense supports role-based access for Finessesupervisors and agents. With role-based access, Finessesupervisors can monitor the recordings of only their respective teams, and Finesses agents can view only their own recordings. To use role-based access, the Finesses AgentInfo gadget should always be active on the desktop of agents and supervisors. Role-based access can only be configured for Finesses-integrated Contact Centers.

For more information on Finesses AgentInfo Gadget, refer Finesses AgentInfo Gadget

The feature supports a set-up with supervisors owning multiple teams. Supervisors can be either the primary or the secondary supervisor for a team. A supervisor can access all recent or active recordings of the teams on the Finesses Search and Play gadget. Supervisors can search for only the MediaSense-associated recordings of agents who belong to the teams for which they are primary or secondary supervisor.
Example

A call is going on between Agent A of Team 1 and Jack. Agent A transfers the call to Agent B of Team 2 and now the call is between Agent B and Jack. The supervisor of Team 1 is able to view the recordings of the call between

• Agent A and Jack
• Agent A and Agent B

However, the supervisor of Team 1 cannot see the recordings of the call between Agent B and Jack as Agent B is not part of the supervisor’s team.

If an agent moves out of the team owned by the supervisor, then the supervisor can access only those recordings of the agent when that agent was part of the supervisor's team. The supervisor cannot access the current recordings of that agent.

MediaSense supports role-based access for active recordings, associated recordings, and archived recordings. To enable Finesserole-based access, check the **Restrict Supervisors to their respective team's recordings only** check box on the **MediaSense Search and Play Configuration** window of **MediaSense Administration** (Administration > Search and Play Configuration).

Note

If the Finesserole-based access feature is enabled, Finessesupervisors will have access to the recordings of their respective teams only. To view all the available recordings in MediaSense Search and Play, the supervisor has to sign in with AXL user credentials.

Related Topics

- Search and Play Configuration, on page 111
- Configuration of AgentInfo Gadget on Finesse Desktop, on page 24

Secured Communication

MediaSense provides secured communication through secure SIP and SRTP (Secure Real-Time Protocol). Secure SIP ensures secured and encrypted SIP signaling between Unified Communications Manager and the MediaSense server. Secure SIP sends SIP messages over a Transport Layer Security (TLS) connection. TLS protects SIP session communications from sniffing. Secure SIP calls flow over trunks created with port 5061.

To support incoming SIP and secure SIP calls, MediaSense now listens on both ports 5060 and 5061, respectively.

SRTP provides decryption of messages passed through the RTP-based communication protocol. SRTP is supported by all nodes in a MediaSense cluster. In case an endpoint is unable to handle SRTP calls, MediaSense will fall back on RTP for call recording.

For secured communication, MediaSense must support the following cipher-message-authentication schemes:

- AES_CM_128_HMAC_SHA1_32
- AES_CM_128_HMAC_SHA1_80
MediaSenses supports SRTP for BiB audio call recordings only.

Certificate Configuration for Secure SIP

Following are the three types of certificate configuration for secure SIP:

- If self-signed certificates are being used, then Tomcat certificate(s) from MediaSense should be uploaded into Cisco Unified Communications Manager as CallManagerTrust certificates and the CallManager certificate(s) should be uploaded into MediaSense nodes as TomcatTrust certificates.

- If CA-signed certificates are being used, then the CA-signed Tomcat certificate(s) from MediaSense and the CA root certificate should be uploaded into Cisco Unified Communications Manager as CallManagerTrust certificates and the CA-signed CallManager certificate(s) and the CA root certificate should be uploaded into MediaSense node(s) as TomcatTrust certificates.

- If CA-signed Tomcat and CallManager CHAIN certificates are being used in MediaSense and Cisco Unified Communications Manager nodes respectively, then there is no need to exchange the certificates among them. The CA-ROOT CHAIN certificate should be uploaded into Cisco Unified Communications Manager as CallManagerTrust certificates and into MediaSense node(s) as TomcatTrust certificates.

Related Topics

Setup Call Control Service Connection, on page 59

Configuration of SIP Trunk Security Profile

To create a SIP trunk security profile for each node of MediaSense, perform the following steps.

Procedure

Step 1  
Access Cisco Unified Communications Manager Administration window and choose System > Security > SIP Trunk Security Profile.

The Find and List SIP Trunk Security Profiles window appears.

Step 2  
Click Add New to create a new SIP trunk security profile.

The SIP Trunk Security Profile Configuration window appears.

Step 3  
Enter the following details:

a) From the Device Security Mode drop-down list, choose Encrypted.

b) From the Incoming Transport Type drop-down list, choose TLS.

c) From the Outgoing Transport Type drop-down list, choose TLS.

Step 3  
In X.509 Subject Name field, enter the value of certificate name present in the tomcat.pem of MediaSense.

Note  
To get the certificate name, go to MediaSense Administration > Cisco Unified OS Administration and choose Security > Certificate Management > tomcat.pem.

For a MediaSense cluster setup, ensure that the X.509 Subject Names of all the MediaSense nodes' certificates are specified separated by a comma and without any white space or a new line.
e) Check the **Transmit Security Status** check box.
f) Click **Save**.

---

**What to do next**

To setup SIP Trunk Security profile. For more information, see the *Setup SIP Trunk Security Profile* section.

---

**Setup SIP Trunk Security Profile**

To set up SIP Trunk security profile, perform the following steps:

**Procedure**

**Step 1**
In **Cisco Unified Communications Manager Administration** window, click **Device > Trunk**.
The **Find and List Trunks** window appears.

**Step 2**
Click **Add New**.
The **Trunk Configuration** window appears.

**Step 3**
From the **Trunk Type** drop-down list, choose **SIP Trunk** and click **Next**.

**Step 4**
In the **SIP Information** section, add a destination row with **Destination Address** as the MediaSense IP address with port 5061.

**Note**
For MediaSense cluster setup, specify the IPs of all the MediaSense nodes with port 5061 in the additional rows in the same trunk.

**Step 5**
From the **SIP Trunk Security Profile** drop-down list, choose the created SIP Trunk Security profile.

---

**Configuration of SRTP for Secured Communication**

To support SRTP along with SIP over TLS, perform the following steps.

**Procedure**

**Step 1**
Go to **Cisco Unified Communications Manager Administration > Device > Trunk > Trunk Configuration**.

**Step 2**
In the Device Information section, check the **SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information** check box.

**Step 3**
From the **Consider Traffic on This Trunk Secure** drop-down list, choose **When using both SRTP and TLS**.

**Note**
Although MediaSense also supports **sRTP only** option but it is not recommended as media encryption key could be exposed at the time of signaling, thus making the security setup vulnerable.
Configuration of Phone Security Profile

To set up phone security profile, perform the following steps:

Procedure

Step 1  On Cisco Unified Communications Manager Administration window, choose System > Security > Phone Security Profile.

The Find and List Phone Security Profiles window appears.

Step 2  Click Add New to create a new phone security profile if there is no security profile for the desired phone.

The Phone Security Profile Configuration window appears.

Step 3  From the Phone Security Profile Type drop-down list, choose a phone security profile type and click Next.

Step 4  In the Phone Security Profile Information section, enter the name of the phone security profile.

Step 5  From the Device Security Mode drop-down list, choose Encrypted.

Step 6  From the Transport Type drop-down list, choose TLS.

Step 7  In the Parameters used in Phone section, enter 5061 as the SIP Phone Port and click Save.

Step 8  On Cisco Unified Communications Manager Administration window, choose Device > Phone.

The Find and List IP Phone Services window appears.

Step 9  Click Add New and from the Phone Type drop-down list, choose the phone type.

Step 10  Click Next.

The Phone Configuration window appears.

Step 11  In the Protocol Specific Information section, choose the phone security profile for this phone type from the Device Security Profile drop-down list.

Configuration on Cisco Unified Communications Manager CLI for Secured Communication

For CTL mixed mode, perform the following steps:

Procedure

Step 1  Open the Cisco Unified Communications Manager CLI prompt and run the command:

  utilsetctl set-cluster mixed-mode

Step 2  Restart Cisco Unified Communications Manager for mixed mode to be effective.
Transport Layer

IPv6 Support

MediaSense supports the latest version of Internet Protocol, Internet Protocol Version 6 (IPv6), which enables data communication over a packet switched network. IPv6 has an advantage over IPv4 with increased address space. IPv6 has 128-bits network address, which is higher in comparison to 32-bits network address of IPv4.

MediaSense supports IPv6 recordings for two-party audio calls as forked by BiB. MediaSense does not support IPv6 for Unified Communications Manager Network-Based recordings and Unified Border Element Dial-Peer forking.

To support endpoints that are IPv4-only, IPv6-only, or dual stack, MediaSense uses ANAT (Alternative Network Address Types) protocol extension to execute IPv6 or IPv4 addresses with Unified Communications Manager. ANAT protocol provides alternate network addresses of different types for a single logical media stream.

Media can be transferred over IPv6 or IPv4 depending on the address family of the endpoint device, however the signaling is done over IPv4 only. MediaSense always gives preference to IPv6 when endpoint is also on dual stack (irrespective of the preferred protocol version in ANAT group). MediaSense recordings made over RTP/IPv6 can be played back and downloaded over IPv4 interfaces.

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.

<table>
<thead>
<tr>
<th>Server or Application Protocol</th>
<th>Server Protocol and Port</th>
<th>Remote Protocol and Port</th>
<th>Remote Device</th>
<th>Used by</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>TCP 443, 8443</td>
<td>Any</td>
<td>Web browser</td>
<td>Administration, serviceability</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP 8440</td>
<td>Any</td>
<td>Client application</td>
<td>API access</td>
</tr>
<tr>
<td>Server or Application Protocol</td>
<td>Server Protocol and Port</td>
<td>Remote Protocol and Port</td>
<td>Remote Device</td>
<td>Used by</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>---------</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP 9443</td>
<td>Any</td>
<td>Client application</td>
<td>Used by media service to redirect authenticated requests.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP 8446</td>
<td>Any</td>
<td>Web browser, API client</td>
<td>Call control service.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP 9081</td>
<td>Any</td>
<td>Client application</td>
<td>Used by media service to redirect authenticated requests.</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP 80, 8080</td>
<td>Any</td>
<td>Web browser</td>
<td>Administration, serviceability</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP 8081</td>
<td>Any</td>
<td>Web browser, API client</td>
<td>Call control service</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP 8085</td>
<td>Any</td>
<td>Another CMS node</td>
<td>Call control service</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP 8087</td>
<td>Any</td>
<td>CMS cluster nodes only</td>
<td>System service</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP 8088</td>
<td>Any</td>
<td>CMS cluster nodes only</td>
<td>Configuration service</td>
</tr>
<tr>
<td>RTSP</td>
<td>TCP 554, 8554</td>
<td>Any</td>
<td>RTSP media player</td>
<td>SM agent</td>
</tr>
<tr>
<td>RTSP</td>
<td>TCP 9554</td>
<td>Any</td>
<td>Client application or media player</td>
<td>Used by media service to redirect authenticated requests.</td>
</tr>
<tr>
<td>RTSP</td>
<td>TCP 8550</td>
<td>Any</td>
<td>Client application</td>
<td>Call control service</td>
</tr>
<tr>
<td>SIP</td>
<td>TCP 5060</td>
<td>TCP 5060</td>
<td>Unified Communications Manager or Unified Border Element</td>
<td>Call control service</td>
</tr>
<tr>
<td>SIP-S</td>
<td>TLS over TCP 5061</td>
<td>TLS over TCP 5061</td>
<td>Unified Communications Manager or Unified Border Element</td>
<td>Call control service</td>
</tr>
<tr>
<td>Server or Application Protocol</td>
<td>Server Protocol and Port</td>
<td>Remote Protocol and Port</td>
<td>Remote Device</td>
<td>Used by</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>---------</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>TCP 1543</td>
<td>Any</td>
<td>CMS cluster nodes only</td>
<td>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.</td>
</tr>
<tr>
<td>Keep-alive heartbeats</td>
<td>UDP 8091</td>
<td>UDP 8091</td>
<td>CMS cluster nodes only</td>
<td>Used by a call control service to detect availability of other call control services.</td>
</tr>
<tr>
<td>JMS</td>
<td>TCP 61610</td>
<td>Any</td>
<td>CMS cluster nodes only</td>
<td>API service</td>
</tr>
<tr>
<td>JMS</td>
<td>TCP 61612</td>
<td>Any</td>
<td>CMS cluster nodes only</td>
<td>Call control service</td>
</tr>
<tr>
<td>JMS</td>
<td>TCP 61616</td>
<td>Any</td>
<td>CMS cluster nodes only</td>
<td>SM agent</td>
</tr>
<tr>
<td>Ephemeral port range</td>
<td>UDP 32768 - 61000</td>
<td>Any</td>
<td>Phone or gateway that sends RTP media streams.</td>
<td>Range of ports used by media service to receive RTP media streams.</td>
</tr>
<tr>
<td>Ephemeral port range</td>
<td>UDP 1024 - 65535</td>
<td>Any</td>
<td>RTSP media player which is being used to listen to an archived or live recording.</td>
<td>Range of local ports used by media service to send RTP media streams.</td>
</tr>
</tbody>
</table>

**Upload and Playback of Prerecorded Media**

**Uploaded Media Files**

MediaSense uploads and plays back video files through SIP signaling control. The video file upload and playback functionalities are used to provide Video-on-Hold and Video-on-Queue features in enterprise and call center deployments. The administrator uploads the media files that must adhere to a given set of...
specifications. The uploaded media files are configured to be used by attaching a unique alphanumeric string to each media file. For more information, see the Media File Management section.

Related Topics
- Media File Management, on page 102

Audio RTSP Playback

MediaSense provides a functionality to create a playlist to be used as an audio playback when a call is in queue or on hold. A playlist is a list of uploaded media files that are played sequentially in a loop. The first media file is picked randomly. The uploaded media files are played back using the RTSP URL. The same URL can be configured on Unified CVP to be used as Interactive Voice Response (IVR) playback when a call is parked until a call center agent is available.

You can add or manage a playlist of audio files using the Playlist Manager window (Cisco MediaSense Administration > Media File Management > Playlist Manager).

Note
The Audio RTSP Playback feature works only with IPv4 (RTSP URL having an IP address and not the hostname).

The feature supports only basic RTSP functionality and not to be used for pause and seek operations.

Related Topics
- Playlist Manager, on page 106
- Add a Playlist, on page 106
- Manage a Playlist, on page 107
MediaSense Installation

- Install MediaSense, on page 35
- Initial Configuration, on page 43
- Upgrade MediaSense, on page 49
- Rollback Cluster, on page 57
- Install COP Files, on page 57
- Language Pack, on page 58

Install MediaSense

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

Preparation

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 Design Guide.

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.

<table>
<thead>
<tr>
<th>Installation Data</th>
<th>Your Entry</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform administrator information</td>
<td>Username:</td>
<td>Information used to sign in to the Unified Communications Operating System Administration and to Cisco Unified Serviceability.</td>
</tr>
<tr>
<td></td>
<td>Password:</td>
<td></td>
</tr>
<tr>
<td>Installation Data</td>
<td>Your Entry</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>MediaSense application administrator information</td>
<td>Username: Password:</td>
<td>Information used to sign in to MediaSense administration and serviceability. You can change the entry after installation by using the CLI commands:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>utils</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>reset_application_ui_administrator_name</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>utils</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>reset_application_ui_administrator_password</code></td>
</tr>
<tr>
<td>MediaSense cluster deployment information</td>
<td>Primary server IP address: Secondary server IP address: Expansion server IP address(es):</td>
<td>If you are unsure of the MTU setting for your network, use the default value of 1500 bytes.</td>
</tr>
<tr>
<td>The MTU size (in bytes) for your network. This setting must be the same on all servers in a cluster.</td>
<td>MTU size:</td>
<td></td>
</tr>
<tr>
<td>Static network configuration</td>
<td>IP Address: IP Mask: Gateway:</td>
<td></td>
</tr>
<tr>
<td>DNS client configuration</td>
<td>Primary DNS: Secondary DNS (optional): Domain:</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td>Hostname or IP address of the NTP server(s):</td>
<td>You must specify at least one valid and reachable NTP server.</td>
</tr>
</tbody>
</table>
### Installation Data

<table>
<thead>
<tr>
<th>Your Entry</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the same security password for all servers in the MediaSense deployment.</td>
<td>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.</td>
</tr>
<tr>
<td>Security password:</td>
<td></td>
</tr>
</tbody>
</table>

### 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, see Cisco Unified Communications Answer File Generator.

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 window may go blank. If the window goes blank:

- Press **Escape** to redisplay the current window and continue the installation.
- Do not press the space bar because this action selects the default option from the current window and moves you to the next window.

The following table describes the actions that the system executes when you press certain keys during installation.

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Press this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move to the next field</td>
<td>Tab</td>
</tr>
<tr>
<td>Move to the previous field</td>
<td>Alt-Tab</td>
</tr>
<tr>
<td>Choose an option</td>
<td>Space bar or Enter</td>
</tr>
<tr>
<td>Scroll up or down in a list</td>
<td>Up and Down arrow</td>
</tr>
<tr>
<td>Return to the previous window</td>
<td>Space bar or Enter to choose Back (when available)</td>
</tr>
<tr>
<td>Get help for a window</td>
<td>Space bar or Enter</td>
</tr>
</tbody>
</table>
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 Design Guide.

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 Design Guide.

• In addition to the approved servers, MediaSense can be installed on a UCS-E module 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 Design Guide. For more information about UCS-E modules, see http://www.cisco.com/en/US/products/ps12629/index.html.

• Virtual machine requirements specific to MediaSense are available at Virtualization for Cisco_MediaSense. For details about virtual machine templates, ESXi, sizing information, and other virtual machine-specific process details, see Unified Communications in a Virtualized Environment.

For more information about hardware limitations, see the Cisco MediaSense Release Notes on Cisco.com (CDC).

Software Requirements

MediaSense must meet the following software requirements:

• The required Unified Communications Manager 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 Design Guide.

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.

Installation

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, 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 web page.

You can install MediaSense from the installation disk and configure it with one DVD insertion. The disk 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. Set up the primary server.

Before you install any secondary or expansion servers, the primary server must be running. The primary server 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 does not provide technical support for systems running in an unsupported mode. To view all VM requirements, visit the Unified Communications Virtualization web page.

- 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 or 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.
The installation may fail if an invalid or incorrect IP address was entered when the MediaSense node was added to the Unified Communications Manager cluster. Refer to Troubleshooting Tips for Cisco MediaSense.

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 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 disk. If your disk 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 disk directly from Cisco Systems.

   • Contact your service provider for assistance.

The Cisco Unified Communications Product Deployment Selection window appears.

Step 4
Click OK on the Cisco Unified Communications Product Deployment Selection window to proceed.

The installation begins.

Step 5
Select Yes if you agree with the displayed information on the Proceed with Install window. If you select No, the installation is canceled.

The screen displays any preexisting version of MediaSense on the hard drive and the version that is available on the disk. 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 in 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 mentioned in the Initial Configuration section.

If you did not provide configuration information in Step 1, and you select Yes in the Proceed with Install window, 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 that apply 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 transmits 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 Primary DNS and Domain. Optional values include 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. Click 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 begin 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 saved to use again when you add a secondary server or an expansion server.
- Can be changed later using the CLI command `set password security`.

Click **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.

Click **OK** and proceed to the next step.

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

**Step 18** Select **Yes** to pause the installation and add the subsequent server information to the primary server. For instructions, see the **MediaSense Server Configuration** section.

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 that you entered for the first server. Click **OK** to continue with the installation.

The **Platform Configuration Confirmation** screen appears.

**Step 20** In the **Platform Configuration Confirmation** screen, click **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

Unmount 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 initial configuration tasks to complete the setup for every node in the cluster.

Related Topics

- Initial Configuration, on page 43
- MediaSense Server Configuration, on page 112

Initial Configuration

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

Procedure

Step 1

Upgrade the VM tools.

For more information on upgrading VM tools, see VMWare Tools.

Step 2

Complete the setup of the primary server. See the Complete Setup for Primary Server section.

Step 3

Add subsequent servers. See the MediaSense Server Configuration section.

Step 4

Complete the setup of each subsequent server. See the Finish Setup for Subsequent Servers section.

Related Topics

- Complete Setup for Primary Server, on page 43
- MediaSense Server Configuration, on page 112
- Finish Setup for Subsequent Servers, on page 46

Complete Setup for Primary Server

The Unified Communications Manager IP address and the Administrative XML Layer (AXL) administrator username and password are required to perform the initial configuration procedure. Access to Unified Communications Manager is required to continue with the MediaSense setup.
The AXL user can only be an end user in Unified Communications Manager.

For Unified Communications Manager 10.0, the AXL user must be configured with the following roles:

- Standard AXL API Access
- Standard CCM Admin Users

For Unified Communications Manager 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 Communications Manager users and roles, see Cisco Unified Communications System Documentation.

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

- Single-Server Deployments
- Dual-Server Deployments
- Three-Server Deployments
- Four-Server and Five-Server Deployments

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 appears.

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

The Service Activation window appears.

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 of the feature services show as enabled in the Service Activation window. After all of 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

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling</td>
<td>This service is in the process of being enabled.</td>
<td>Wait for the state to moved to the Enabled.</td>
</tr>
<tr>
<td>Enabled</td>
<td>This service is now fully turned on and ready to</td>
<td>Wait until all the feature services for this server reach the Enabled</td>
</tr>
<tr>
<td></td>
<td>function.</td>
<td>state. The primary server requires all feature services to be enabled.</td>
</tr>
<tr>
<td>Error</td>
<td>The system cannot enable this service due to an</td>
<td><strong>Warning</strong> If the Database service or the feature services are not enabled, the system does not allow you to proceed with the setup procedure.</td>
</tr>
<tr>
<td></td>
<td>error.</td>
<td>Your response depends on the service that failed to be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If it is the database service or the configuration service that failed, you must first correct the error and restart the initial setup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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 is not fully in service until you fix these issues.</td>
</tr>
</tbody>
</table>

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

**Step 4**

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

**Note** You cannot change the password for the AXL user in the MediaSense application. The MediaSense application only authenticates the password configured in Unified Communications Manager. You can, however, modify the AXL server IP address.

**Note** MediaSense accepts passwords upto 20 characters in length. So the AXL password should not exceed 20 characters.

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** window appears.

**Step 5**

If the client applications using MediaSense need to make outbound recording calls, provide the Unified Communications Manager server IP address for the call control service on the **Call Control Service Provider** window.
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 Communications Manager 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 Communications Manager Administration, configure the SIP trunk, route group, route list, and recording profile.

When you finish the initial configuration process for any MediaSense server, you must access the Unified Communications Manager server for your deployment (based on the information provided during the installation and initial configuration process).

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 by using the MediaSense Administration user interface.

**Related Topics**
- Single-Server Deployments, on page 9
- Dual-Server Deployments, on page 10
- Three-Server Deployments, on page 11
- Four-Server and Five-Server Deployments, on page 12
- Select AXL Service Providers, on page 91
- Setup Call Control Service Connection, on page 59
- MediaSense Server Configuration, on page 112

**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 Installation process.

Note: If you have ever increased the size of the /uploadedMedia partition on your system, after you install a new node you 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 the Media Partition Management section.

**Related Topics**
- Installation, on page 39
- Media Partition Management, on page 113

**Finish Setup for Subsequent Servers**

The Unified Communications Manager IP address and the Administrative XML Layer (AXL) administrator username and password are required to perform the initial configuration procedure. You need to have access to Unified Communications Manager to continue with the MediaSense setup.

See the following sections to review the considerations for your intended deployment:
- Single-Server Deployments
- Dual-Server Deployments
- Three-Server Deployments
- Four-Server and Five-Server Deployments

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 the MediaSense Administration section.

Procedure

Step 1

After you complete the installation procedure specified in the Install MediaSense and Unified OS section, 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.

  After 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:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Database service</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Configuration service</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>API service</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Media service</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Call control service</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SM Agent</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Select the server type and click **Next**. The **Service Activation** window 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.

---

**Related Topics**

- Single-Server Deployments, on page 9
- Dual-Server Deployments, on page 10
- Three-Server Deployments, on page 11
- Install MediaSense and Unified OS, on page 39
- Cisco MediaSense Administration, on page 89

---

**Confirming MediaSense Operation**

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

- Sign in to MediaSense Administration on each server. See the **MediaSense Administration** section.
- Sign in to MediaSense Serviceability Administration on each server. See the **MediaSense Serviceability** section.
- Services described in Setup Summary that are enabled on each server. For status description, see the **Complete Setup for Primary Server** section.

---

**Note**

After the MediaSense cluster installation process is complete, install the COP (ciscocm.mediasense_swap_increase.11.x.k3.cop.sgn) to increase the swap memory from 2GB to 6GB.

You can download the COP file from the software download page: [https://software.cisco.com/download/home/283613140/type/284140547/release/Security_Patches](https://software.cisco.com/download/home/283613140/type/284140547/release/Security_Patches)

**Related Topics**

- Cisco MediaSense Administration Menu, on page 89
- Access Cisco MediaSense Administration, on page 90
- Unified Communications Manager Configuration, on page 90
- Cisco Finesse Configuration, on page 93
- MediaSense API User Configuration, on page 95
- Prune Policy Configuration, on page 97
- Incoming Call Configuration, on page 99
- Media File Management, on page 102
- Archival, on page 108
- Search and Play Configuration, on page 111
- MediaSense Administration System, on page 112
Upgrade MediaSense

You can upgrade to MediaSense Release 11.x(x) directly from Release 10.x. If you are running an earlier release, you may have to upgrade more than once to bring your system up to the current release.

Upgrade Path

The following table lists the supported paths to upgrade to Cisco MediaSense 11.x(x).

<table>
<thead>
<tr>
<th>Current Version</th>
<th>Upgrade Path</th>
<th>Description</th>
</tr>
</thead>
</table>
<pre><code>           | 2. Then upgrade directly from Release 10.x to Release 11.x(x). | A Cisco Options Package (COP) file is required to perform an upgrade from Release 9.1(1) to Release 10.0(1) or 10.5(1). A COP file provides a generic method to deploy Cisco software outside the normal upgrade process. |
</code></pre>
<p>| Release 10.x    | Upgrade directly to Release 11.x(x). | This is a refresh upgrade as the RHEL version of the MediaSense operating system changes in Release 11.x(x). |</p>

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

Upgrading MediaSense from versions prior to 10.5 to 10.5 (including its ES and SU releases) or 11.0 (including any ES & SU) will fail if the RecordingSession table has more than 2.5 million records unless a workaround is applied. For more information on the workaround, refer to https://bst.cloudapps.cisco.com/bugsearch/bug/CSCup30602/?reffering_site=dumpr.

A node can take several hours to upgrade depending on the number and size of recordings it holds. When you upgrade a node with very large data sets, it takes around 90 additional minutes per 1 million recordings.

In case of Cisco Finesse configuration, if you are upgrading to MediaSense Release 11.5(1), you must
- Change the IP address or hostname of Finesse server to FQDN (fully qualified domain name) as Finesse is configured with an IP address.
- Exchange the tomcat trust certificate between MediaSense and Unified CCX servers. For more information, refer the Cisco Finesse Configuration section.
Upgrade Considerations

Consider these guidelines when you upgrade MediaSense:

- **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.

- **Rollback to Previous Version**—If you have taken a VM snapshot of each node before initiating an upgrade, you can revert to a previous software version that was running before the upgrade. However, MediaSense does not support the CLI Command, `utils system switch-version`, to revert to the older version.

  ![Note](image)

  There is no other way to rollback to the previous version.

- **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 lose these configuration changes.

  ![Note](image)

  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**—Remember to install any required COP files (including the language pack COP) after each upgrade.

When upgrading from previous releases, consider this information:

• 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 required 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 Release 9.0(1) to 9.1(1) or 10.0(1) and then want to add nodes to your cluster, be aware that although the new nodes are installed with expandable recorded media storage, we do 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.

**Virtual Machine Parameters Settings for Refresh Upgrade**

Before you perform a refresh upgrade to 11.x, you must modify the following virtual machine parameters:

• Red Hat Enterprise Linux version

• Network Adapter

• Memory

**Procedure**

1. **Step 1**
   From **VMware VSphere Client**, right-click the virtual machine and select the **Power Off** option.

2. **Step 2**
   Click the **Edit Settings** tab.
   The Virtual Machine Properties window appears.

3. **Step 3**
   In the **Options** tab, select **General Options** and update the **Guest Operating System** from Red Hat Enterprise Linux 4 (32-bit) to Red Hat Enterprise Linux 6 (64-bit).

4. **Step 4**
   In the **Hardware** tab, click **Add**.
   The Add Hardware window appears.

5. **Step 5**
   In the Add Hardware window, select **Device Type > Ethernet Adapter** and click **Next**.

6. **Step 6**
   In the Adapter Type area, choose **VMXNET3** from the Type drop-down list and click **Finish**.

7. **Step 7**
   To remove the existing adapter, under the Hardware tab, select **Network Adapter 1** and click **Remove**.
Step 8  
Click OK.

Step 9  
If you are using a 2vCPU Virtual Machine, perform the following steps to increase the memory from 6 GB to 8 GB before the refresh upgrade:

a)  In the Hardware tab, click Memory.

b)  In the Memory Configuration pane on the right window, increase the Memory Size to 8 GB, and then click OK.

Step 10  
Power on the virtual machine and continue with the refresh upgrade.

Upgrade Cluster to Release 11.x(x)

This procedure describes a cluster where one or more individual nodes (servers) are upgraded. To upgrade individual nodes, see the Node Upgrade Procedures section.

For Release 11.x(x), customers should upgrade their hosts to a newer version of ESXi that is supported before they can upgrade to MediaSense Release 11.x(x).

If you are running an earlier release of MediaSense, you must upgrade to Release 9.1(1) before you can upgrade to Release 11.x(x). Refer to the Cisco MediaSense User Guide for Release 9.1(1) to upgrade to Release 9.1(1) before using the procedure in this document to upgrade to Release 11.x(x).

For Release 11.5(1), if you are upgrading MediaSense configured with Cisco Finesse, consider the following:

• Change the IP address or hostname of Finesse server to FQDN (fully qualified domain name) as Finesse is configured with an IP address.

• Exchange the tomcat trust certificate between MediaSense and Unified CCX servers. For more information, refer the Cisco Finesse Configuration section.

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 Design Guide.

• 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.

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.

On an upgrade to Release 11.x(x), the following message appears:

Partitions are unaligned, however this does not have a functional impact.

You can ignore the message as it does not have an impact on MediaSense functionality and performance.
Procedure

Step 1  Take a VM snapshot of each node.
Step 2  Upgrade the primary node and wait for it to restart. (See the Node Upgrade Procedures section.)
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  After all of the nodes have been successfully upgraded, delete the VM snapshot on each node.

Related Topics
  Node Upgrade Procedures, on page 53

Node Upgrade Procedures

This section provides procedures for upgrading nodes using software from these sources:

- Local source
- Remote sources using either the command line interface (CLI) or Unified OS Administration

Upgrade Nodes From a Local Source

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 takes these actions:

- Upgrades to the release specified.
Remote Sources

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 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 1 GB 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
- Cygwin
- Titan

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

- Upgrade Nodes Using Unified OS Administration
- Upgrade Nodes Using Unified OS CLI

Related Topics

Upgrade Nodes Using Unified OS Administration, on page 54  
Upgrade Nodes Using Unified OS CLI, on page 55

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 the Upgrade Nodes Using Unified OS CLI section.

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.

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 take these actions:

- Upgrades to the release specified.
- Switches versions and reboots.
- Starts taking calls.

---

**Related Topics**

Upgrade Nodes Using Unified OS CLI, on page 55

---

**Upgrade Nodes Using Unified OS CLI**

**Note**

You can also use the web interface of 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.

**Procedure**

**Step 1**

Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.
**Upgrade Nodes Using Unified OS CLI**

**Step 2** Sign in to the Unified OS console. See CLI Access, on page 141 for more information.

**Step 3** Enter `utils system upgrade initiate` at the CLI prompt.

The following options appear in the window:

- 1) Remote Filesystem Via SFTP
- 2) Remote Filesystem Via FTP
- 3) DVD/CD
- 4) 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 takes these actions:

- Upgrades to the release specified.
- Switches versions and reboots.
- Starts taking calls.

---

**What to do next**

After the MediaSense cluster upgrade process is complete, install the COP (cisco.mediasense_swap_increase.11.x.k3.cop.sgn) to increase the swap memory from 2GB to 6GB.

You can download the COP file from the software download page: https://software.cisco.com/download/home/283613140/type/284140547/release/Security_Patches
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 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.
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.

 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 the Upgrade Nodes From a Local Source section. (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 the Remote Sources section. (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.

 Related Topics

 Upgrade Nodes From a Local Source, on page 53
 Remote Sources, on page 54

 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 the Install COP Files section to install the language you want on your interface.

 Related Topics

 Install COP Files, on page 57
Advanced Tasks

- Unified Communications Manager Provisioning for MediaSense, on page 59
- MediaSense Setup with Cisco Unified Border Element, on page 61
- Server IP Address Changes, on page 70
- Storage Management Agent, on page 80
- Answer Files for Unattended Fresh Installations, on page 86
- Disable iLBC, iSAC and Opus for Recording Device, on page 86
- Reorder the G.722.1 Codecs, on page 86

Unified Communications Manager Provisioning for MediaSense

When you finish the initial configuration process for any MediaSense server, you must access the Unified Communications Manager server for your deployment (based on the information provided during the installation and initial configuration process).

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

Setup Call Control Service Connection

The call control service in MediaSense is referred to as a SIP trunk in the Cisco Unified Communications Manager interface and documentation. In Cisco Unified Communications Manager 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 Cisco Unified Communications Manager Administration.

**Note**

Be sure to configure Cisco Unified Communications Manager 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 Cisco Unified Communications Manager, you will need to provide this IP address in the Call Control Service Provider Configuration panel of the **Cisco Unified CM Configuration** window in Cisco MediaSense Administration.

Even if already enabled, the call control service is not in service until you have configured the call control service provider.
Use this procedure to configure the SIP trunk information in Cisco Unified Communications Manager if your installation calls for Built-in-Bridge (BiB) recording or Network-based Recording (NBR).

**Procedure**

**Step 1**
Invoke and connect to the Cisco Unified CM Administration web interface using a valid Unified Communications Manager 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 the Cisco Unified CM Administration web page.

Follow the procedure specified in Cisco Unified Communications Manager 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 on the Cisco Unified CM Administration web page. Follow the procedure specified in the Unified Communications Manager Administration documentation to add a new SIP trunk.

For non-secure mode, perform the following steps to configure the device.

a) In the Device Information section, enter the device name in the Device Name field and choose the device pool from the Device Pool drop-down list.
b) Assign SIP information.
c) In the SIP Information section, enter the destination IP address, destination IPv6 address, and port (5060) for MediaSense.
d) Select the SIP trunk security profiles and SIP profile (created in Step 2)
e) Ensure that the Media Termination Point Required check box is unchecked.
f) Near the bottom of the screen, select the Run On All Active Unified CM Nodes check box.
g) Save this configuration.

For secure mode, perform the following steps to configure the device.

a) In the Device Information section, enter the device name in the Device Name field and choose the device pool from the Device Pool drop-down list.
b) In the Device Information section, check the SRTP Allowed check box and from the Consider Traffic on this Trunk Secure drop-down list, choose the When using both sRTP and TLS option.
c) In the SIP Information section, enter the destination address, destination IPv6 address, and port (5061) for MediaSense.

**Note**
Click the Add icon to add IP addresses of additional nodes of the MediaSense cluster as destination addresses in the trunk.

d) From the SIP Trunk Security Profile drop-down list, choose the SIP Trunk security profile that you want to map with the trunk.

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

**Note**
For NBR, in the Recording Information section, select the This trunk connects to a recording-enabled gateways radio button.

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

Follow the procedure specified in the Unified Communications Manager 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 on the Cisco Unified CM Administration web page.

Follow the procedure specified in your Cisco Unified Communications Manager 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.

**Note** For NBR, select Gateway Preferred in the Recording Media Source drop-down list.

---

**MediaSense Setup with Cisco Unified Border Element**

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

**Manage Unified Communications Manager Users**

The Administrative XML Layer (AXL) authentication allows you to enter the Unified Communications Manager cluster and retrieve the list of Unified Communications Manager servers within a cluster. During the AXL authentication, if the Unified Communications Manager Publisher is offline or not available, you can provide the next available Unified Communications Manager Subscriber for the AXL authentication. The AXL Administrator username may not be same as the Unified Communications Manager Administrator username for that cluster. Be sure to add the username for the AXL Administrator to the Standard Unified...
Communications Manager Administrators group and Standard AXL API Access roles in Unified Communications Manager.

Do the following tasks before you start using MediaSense servers for a Unified Border Element deployment:

**Procedure**

- Configure and deploy the required Unified Communications Manager cluster and users before you configure MediaSense. For more information, see the Unified Communications Manager documentation.
- Review the Supported Deployments section for information about Unified Communications Manager authentication.
- Ensure that you have the Unified Communications Manager IP address, AXL Admin username, and AXL Admin Password that you need to complete the MediaSense initial configuration tasks.

**Cisco MediaSense Provisioning for Unified Border Element**

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

⚠️ **Caution**

To enhance interoperability with third-party SIP devices, Unified Border Element 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 Unified Border Element deployment:

- Select AXL Service Providers
- Replace Unified Communications Manager Service Providers
- Provision Users for MediaSense Deployment

**Note**

You do not need to configure call control service providers in MediaSense for any Unified Border Element deployment.

**Related Topics**

- Select AXL Service Providers, on page 91
- Replace Unified Communications Manager Service Providers, on page 92
- MediaSense API User Configuration, on page 95

**Unified Border Element and MediaSense Setup**

The Unified Border Element application uses the CLI to access and configure Unified Border Element to enable media recording in MediaSense.

Complete the tasks identified in this section to access and configure Unified Border Element for MediaSense:
Unified Border Element Gateway Accessibility

To access Unified Border Element, 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 Unified Border Element administrator. For more information, see the following table and the Unified Border Element documentation.

Table 3: Unified Border Element Access Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>An IP address for the Unified Border Element gateway.</td>
</tr>
<tr>
<td>Username</td>
<td>Username configured on the gateway device.</td>
</tr>
<tr>
<td>Password</td>
<td>Password configured for this user name.</td>
</tr>
</tbody>
</table>

Unified Border Element View Configuration Commands

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

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

Table 4: Cisco IOS Commands to View Unified Border Element Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Displays the existing configuration for this Unified Border Element gateway.</td>
</tr>
<tr>
<td>show startup-config</td>
<td>Displays the startup configuration for this Unified Border Element gateway.</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the IOS version being used in this Unified Border Element gateway.</td>
</tr>
</tbody>
</table>
Global-Level Interoperability and MediaSense Setup

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

Set Up Global Level

Procedure

**Step 1**  Connect to your Unified Border Element 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
```

**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 Unified Border Element and Unified Border Element 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)# asymmetric 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 Unified Border Element.

**Step 6**  At this point, you will need to save the Unified Border Element configuration and reboot Unified Border Element.

**Caution**  Be sure to reboot Unified Border Element during off-peak hours.

a)  Save your Unified Border Element configuration.

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show call active voice summary</td>
<td>Displays the number of active SIP calls.</td>
</tr>
</tbody>
</table>
cube# copy run start

b) Reboot Unified Border Element.

cube# reload

Step 7 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 1
cube(config)# codec preference 1 mp4a-latm fmtp-select-one max-bitrate 64000
cube(config)# codec preference 2 g711ulaw
cube(config)# codec preference 3 g729br8
cube(config)# codec preference 4 g722-64
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 8 Create video media profile and media class.

cube(config)# media profile video 1
cube(config)# ref-frame-req rtcp retransmit-interval 50 retransmit-count 0
cube(config)# ref-frame-req sip-info
cube(config)# media class 2
cube(config)# video profile 1
cube(config)# media class 3
cube(config)# recorder parameter
cube(config)# media-recording 3000

Step 9 To simplify debugging, you must synchronize the local time in Unified Border Element 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 Unified Border Element:

cube(config)# ntp update-calendar
cube(config)# snntp server 10.10.10.5

---

**Dial-Peer Level Setup**

**Note**

This information describes a sample configuration. Unified Border Element may be deployed in multiple ways.

Each MediaSense deployment for Unified Border Element 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.

Figure 7: Dial-Peer Level Setup

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

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

Set Up Unified Border Element 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 Unified Border Element documentation. It is a tutorial to provide detailed information about configuring Unified Border Element for MediaSense. For the latest information, see Unified Border Element documentation.

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 9700
```

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 the Set Up Global Level section). In this example, the number media class is 219.

```
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 9700.
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

c) 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 the Set Up Global Level section). In this example, the number media class is 2.

cube(config-dial-peer)# media-class 2

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

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

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

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

cube(config-dial-peer)# exit

cube(config)# exit

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 Unified Border Element 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 1234.

cube(config-dial-peer)# destination-pattern 1234

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 Unified Border Element 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 Unified Border Element 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 Unified Border Element 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 Unified Border Element configuration.

cube# copy run start

Related Topics

Set Up Global Level, on page 64
Unified Border Element Deployments Log Commands

Cisco Unified Border Element (Unified Border Element) 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>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>service timestamp debug datetime msec localtime show-timezone</code></td>
<td>Specifies the millisecond (msec) timestamp for various debug events.</td>
</tr>
<tr>
<td><code>service timestamps log datetime msec localtime show-timezone</code></td>
<td>Specifies the millisecond (msec) timestamp for various log events.</td>
</tr>
<tr>
<td><code>localtime logging buffered 1000000</code></td>
<td>Specifies the memory allocation for Unified Border Element logins.</td>
</tr>
<tr>
<td><code>no logging rate-limit</code></td>
<td>Specifies that all log messages should be logged.</td>
</tr>
<tr>
<td><code>no logging console</code></td>
<td>Specifies that log messages should not be displayed on the console.</td>
</tr>
</tbody>
</table>

Table 5: Useful Log Commands for Unified Border Element Deployments

Server IP Address Changes

You may want to change the IP address of a MediaSense server in several scenarios, including moving a server from one segment to another or resolving a duplicate IP address issue.

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 an 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 IP addresses or 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, enter 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, enter 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 the installation of the subscriber.
- 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:**
Change IP Address of Primary Server

Change IPv4 Address of Primary Server

Warning

Using this procedure disrupts all services. Be sure to use it only during a scheduled downtime.

To successfully change the IP address, you must complete all steps in this procedure.

Procedure

Step 1

Review and address the instructions listed in the Prepare for IP Address Change section before changing the IP address on any Cisco 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, enter 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  Point every server in the cluster to the new primary’s IP address by entering the **set network cluster primary ip** command from each server in the Cisco 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 5  If you are moving the primary server to a different subnet that requires a new default gateway address, change the default gateway by entering the **set network gateway** command from the primary server:

**Example:**

```
set network gateway 10.3.90.2
*** WARNING ***
This will cause the system to temporarily lose network connectivity
Continue (y/n)? y
trying to restart network...
```

**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 6  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
*** WARNING ***
This command will restart system services
```

**Note:** Please verify that the new ip address is unique across the cluster and, if DNS services are utilized, any DNS configuration is completed before proceeding.

```
Continue (y/n)? y
```

This command changes the IP address and reboots the primary server.

Step 7  Type **Yes** and press **Enter**.

Step 8  Verify the cluster configuration by entering the **show network cluster** command on all other servers.

**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.
Step 9  
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 10  
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:**

```bash
utils network host mcs-pri
Hostname mcs-pri resolves to 10.10.10.135

show tech network hosts
```

```
/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 11  
Verify the cluster configuration by issuing the `show network cluster` command.

**Example:**

```bash
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.

**Related Topics**  
- Prepare System for IP Address Change, on page 70

**Change IPv6 Address of Primary Server**

You can change the IPv6 address of a server in various scenarios, such as while moving a server from one segment to another or resolving a duplicate IPv6 address issue.

To change the IPv6 address, run the `set network ipv6 static_address <ipv6> <netmask>` CLI command in the command prompt.

For example:

```bash
set network ipv6 static_address 2001:db8:1234:77:50 64
```
Change IP Address of Secondary Server

Change IPv4 Address of Secondary Server

This procedure disrupts all services. Be sure to make any changes during a scheduled downtime.

To successfully change the IP address, you must complete all steps in this procedure.

Procedure

Step 1
Review and address the instructions listed in the Prepare System for IP Address Change section before changing the IP address on any MediaSense server.

Step 2
From the primary server, enter 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
```

Step 3
Point every server in the cluster to the new secondary server IP address by entering 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 4
If you are moving the secondary server to a different subnet that requires a new default gateway address, change the default gateway by entering the `set network gateway` command from the secondary server.

Example:

```
set network gateway 10.3.90.2
*** WARNING ***
This will cause the system to temporarily lose network connectivity
Continue (y/n)? y
trying to restart network...
```

Step 5
Type Yes and press Enter.

Step 6
From the secondary server, enter 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
```
*** WARNING ***
This command will restart system services

Note: Please verify that the new ip address is unique across the cluster and, if DNS services are utilized, any DNS configuration is completed before proceeding.

============================================
Continue (y/n)? y

Step 7 Verify the cluster configuration by entering the show network cluster command on all other servers.

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
```

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.

Step 8 Reboot all servers in the Cisco 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 9 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 10 Verify the interim cluster configuration by entering 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
```
Change IPv6 Address of Secondary Server

For IPv6 address change of a secondary server, refer the Change IPv6 Address of Primary Server section.

Related Topics
  - Change IPv6 Address of Primary Server, on page 74

Change IP Address of Expansion Server

This procedure disrupts all services. Make any changes only during a scheduled downtime.

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 70 before changing the IP address on any server.

Step 2
From the CLI of the primary server, enter 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
```

Successful

Step 3
If you are moving the expansion server to a different subnet that requires a new default gateway address, change the default gateway by entering the `set network gateway` command from the expansion server.

Example:

```
set network gateway 10.3.90.2
```

*** WARNING ***
This will cause the system to temporarily lose network connectivity
Continue (y/n)? y
trying to restart network...
**Step 4**  From the expansion server, enter 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
```

*** WARNING ***
This command will restart system services

Note: Please verify that the new ip address is unique
across the cluster and, if DNS services are
utilized, any DNS configuration is completed
before proceeding.

Continue (y/n)? y

This command changes the IP address and re-boots the expansion server.

**Step 5**  Type Yes and press Enter.

**Step 6**  Verify the cluster configuration by entering the `show network cluster` command on all other servers.

**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.cisco.com 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 7**  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 8**  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 9**  Verify the cluster configuration by entering 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

Related Topics
Prepare System for IP Address Change, on page 70

Change IPv6 Address of Expansion Server

For IPv6 address change of an expansion server, refer the Change IPv6 Address of Primary Server section.

Related Topics
Change IPv6 Address of Primary Server, on page 74

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 enter 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 the Prepare System for IP Address Change section before changing the IP address on any MediaSense server.

Step 2
From the primary server, issue the following commands:

```
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, enter the following commands:

set network cluster primary ip <primary new ip>
set network cluster secondary ip <secondary new ip>

**Step 4**
From the expansion server, enter the following commands:

set network cluster primary ip <primary new ip>
set network cluster secondary ip <secondary new ip>

**Step 5**
From the primary server, enter the following command:

run sql select name,nodeid from ProcessNode

**Step 6**
From the secondary server, enter the following command:

run sql select name,nodeid from ProcessNode

**Step 7**
From the expansion server, enter the following command:

run sql select name,nodeid from ProcessNode

**Step 8**
From the primary server, enter the following commands:

set network gateway (if required)
set network ip eth0 <primary new ip> <address mask> <gw>

**Step 9**
From the secondary server, enter the following commands:

set network gateway (if required)
set network ip eth0 <secondary new ip> <address mask> <gw>

**Step 10**
From the expansion server, enter the following commands:

set network gateway (if required)
set network ip eth0 <expansion new ip> <address mask> <gw>

**Step 11**
From each server in the MediaSense cluster, enter the following commands to verify the cluster configuration.

utils network host
show tech network hosts
show network cluster

### Related Topics

Prepare System for IP Address Change, on page 70

---

### 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.
Storage Threshold Values and Pruning Avoidance

An API event (an alert) is issued each time the media disk space (which stores the recorded media) reaches various thresholds. It is important to monitor the threshold alerts because if the disk space reaches a certain threshold, MediaSense may automatically prune the recordings (priority mode recording) or may not save the recordings (retention mode recording).

There are two ways that you can avoid losing recordings:

**Retention Mode:** You can uncheck the *Automatically prune recordings after they are more than ___ days old, and when disk space is needed for new recordings* check box and follow all threshold alerts by manually deleting unwanted recordings. By doing so, you will not lose any recordings unless you purposely remove the recordings. Be careful to follow the RTMT disk space alerts and remove recordings when need so that you do not lose new recordings that come into the server when the disk space is too high.

**Priority Mode:** You can check the *Automatically prune recordings after they are more than ___ days old, and when disk space is needed for new recordings* check box and then save the required recordings as MP4 files to a safe location in your network using the MediaSense Archival feature. Check the check box if the priority is to record new calls that come to the MediaSense server as compared to making sure to never prune old recordings. Archiving ensures that you do not lose the older recordings once the recordings are deleted from the MediaSense server.

For more information about these options, see the *Prune Policy Configuration* section.

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

**Table 6: Storage Threshold Values**

<table>
<thead>
<tr>
<th>Threshold Storage</th>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTER_LOW_STORAGE_SPACE</td>
<td>Recorded media crossed the 75%</td>
<td>First warning to indicate that the disk storage is running into low space</td>
</tr>
<tr>
<td></td>
<td>storage utilization mark.</td>
<td>condition.</td>
</tr>
<tr>
<td>EXIT_LOW_STORAGE_SPACE</td>
<td>Recorded media usage dropped</td>
<td>The disk storage is exiting the low storage space condition.</td>
</tr>
<tr>
<td></td>
<td>below 70% utilization mark.</td>
<td></td>
</tr>
<tr>
<td>Threshold Storage</td>
<td>Percentage</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ENTER_CRITICAL_STORAGE_SPACE</td>
<td>Recorded media crossed the 90% local storage utilization mark.</td>
<td>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 pruning based on the age of the recordings), new recording sessions are not accepted when you reach this threshold. If the disk space usage exceeds 96%, the old recordings are deleted in a batch of 200 recordings (oldest first). After every batch deletion, the system checks the disk space usage. If the disk space usage comes below 96%, then the deletion process stops. After this point, you will need to manually purge recordings to get below the 90% threshold to start recordings again. If operating in the new recording priority mode and the disk space usage exceeds 86% (to make room for new recordings), the older recordings are subject to automatic deletion in a batch of 200 recordings (oldest first). Pruning still takes place as per the specified days in the MediaSense Prune Policy Configuration window (Cisco MediaSense Administration &gt; Prune Policy Configuration), however, these two pruning are independent of each other. After every batch deletion, the system checks the disk space usage. If the disk space usage comes below 86%, then the deletion process stops. In this way, the system automatically deletes the recordings so that the administrator does not have to remove the recordings manually.</td>
</tr>
<tr>
<td>Threshold Storage</td>
<td>Percentage</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EXIT_CRITICAL_STORAGE_SPACE</td>
<td>Recorded media usage dropped below 85% utilization mark.</td>
<td>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.</td>
</tr>
<tr>
<td>ENTER_EMERGENCY_STORAGE_SPACE</td>
<td>Recorded media crossed the 99% storage utilization mark.</td>
<td>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.</td>
</tr>
<tr>
<td>EXIT_EMERGENCY_STORAGE_SPACE -</td>
<td>Recorded media usage dropped below the 97% utilization mark.</td>
<td>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.</td>
</tr>
</tbody>
</table>

See the MediaSense Developer Guide 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

- storageThresholdEvent Recording Event

Related Topics

Prune Policy Configuration, on page 97
System Thresholds

Storage Management agent (SM agent) monitors the storage thresholds 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 if it is reachable by using the `ping` command.

For more information about threshold value percentages, see the **Storage Threshold Values and Pruning Avoidance** section.

**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.

**Related Topics**

- **Storage Threshold Values and Pruning Avoidance**, on page 81

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
<?xml version="1.0" encoding="UTF-8" ?>
```
The number of media partitions directly corresponds to the number of configured media disks. If you configure two media disks, you see two partitions: /media1 and /media2.

### Storage Use Information Obtained by Using Unified RTMT and Cisco Prime Collaboration Assurance

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.

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

Unified RTMT and Cisco Prime Collaboration Assurance display 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.

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 and Cisco Prime Collaboration Assurance.

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.
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, see Cisco Unified Communications Answer File Generator.

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

Disable iLBC, iSAC and Opus for Recording Device

Caution MediaSense does not support Internet Low Bitrate Codec (iLBC), Internet Speech Audio Codec (iSAC) or Opus Interactive Audio Codec. Consequently, you must disable these features in Unified Communications Manager before you proceed with the MediaSense configuration.

Procedure

1. Invoke and connect to the Unified CM Administration web interface using a valid Unified Communications Manager username and password.
2. Select System > Service parameters in Unified CM Administration.
3. On the Service Parameter Configuration web page, select the required server and service (Cisco CallManager) from the Select Server and Service drop-down list.
4. Go to the Cluster-wide Parameters (Location and Region) section and locate the iLBC Codec Enabled parameter, iSAC Codec Enabled parameter and the Opus Codec Enabled parameter.
5. Set the value for both of these parameters as Enable for All Devices Except Recording-Enabled Devices and save your configuration.

Reorder the G.722.1 Codecs

Caution MediaSense does not support the G.722.1 codecs, which are not the same as G.722. However, you cannot disable the G.722.1 codecs in Cisco Unified Communications Manager.
For recording Jabber-to-Jabber calls (clients with BiB) where one of these is either a Mac or Windows Jabber client, you must place G722.1 codecs lower than all the G711 and G729 codecs in the Audio Codec Preference List Configuration window of Cisco Unified Communications Manager. To do this, see the Edit Audio Codec Preference List section of the Cisco Unified Communications Manager Administration Guide.
Reorder the G.722.1 Codecs
Cisco MediaSense Administration Menu

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 Communications Manager 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, select Help > This Page.
  
  - To verify the version of the administration running on the server, select 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, select 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, select Help > Troubleshooting Tips.
    
    If you are connected to the external network, this link connects you to the Trouble Shooting page for Cisco MediaSense.
You will be logged out from the MediaSense Administration interface if the session remains idle for 120 minutes.

**Access Cisco 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 or Server FQDN>/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.

*Note* 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.

**Unified Communications Manager Configuration**

This section pertains to a Unified Communications Manager cluster and assumes that the user has both Unified Communications Manager and MediaSense administrator privileges.

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 *Initial Configuration* section.

*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.

**Related Topics**

- **Initial Configuration**, on page 43
Select AXL Service Providers

During the MediaSense initial configuration setup process, you may have provided the AXL information for the primary server. If you did not provide this information during the initial configuration 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 Communications Manager 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.

Note MediaSense accepts passwords up to 20 characters in length. So the AXL password should not exceed 20 characters.

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 Communications Manager server, ensure that the server you select is a valid Unified Communications Manager call control server. The servers in the Available list may include Cisco Unified Presence servers as well as Unified Communications Manager 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 **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 Communications Manager server from the Selected list box, a browser window pops up informing you about the deselected servers.

*Caution* If you modify the Unified Communications Manager cluster and do not select the required call control service providers for the new Unified Communications Manager 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 Communications Manager Service Providers

In the Unified Communications Manager Configuration web page, you can select Unified Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 **AXL Service Provider Configuration** section 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 Communications Manager 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 Communications Manager IP address in this page, the other service provider IP addresses in this Unified Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager cluster and do not select the required call control service providers for the new Unified Communications Manager 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 Communications Manager 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 **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.

---

**Cisco Finesse Configuration**

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

Use the Cisco Finesse Configuration window to identify the primary and secondary Finesse server fully qualified domain names for MediaSense to use for user authentication against Finesse. IP addresses cannot be used.
Procedure

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

Step 2 In the Primary Cisco Finesse FQDN field, enter the FQDN (fully qualified domain name) of the Finesse server that you want as the primary server for MediaSense to communicate with.

Step 3 (Optional) In the Secondary Cisco Finesse FQDN field, enter the FQDN of the Finesse server that you want as the secondary server for MediaSense to communicate with.

Note 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.

Step 5 If CA signed certificates are used on MediaSense and Unified CCX servers, skip step 6.

The configuration of Finesse with MediaSense is complete.

Step 6 (Optional) If self-signed certificates are used on both MediaSense and Unified CCX, then you must upload MediaSense tomcat certificate to Tomcat trusted store of Unified CCX server and Cisco Finesse tomcat certificate to Tomcat trusted store of MediaSense.

For more information on how to upload self-signed certificates, refer the Upload Cisco MediaSense Certificate to Unified CCX Server section of the Cisco Unified CCX Administration Guide and the Upload Unified CCX Certificate to Cisco MediaSense Server section of this guide.

Step 7 Restart MediaSense and Unified CCX servers to establish the connection.

What to do next
Restart MediaSense and Unified CCX servers to establish the connection.

Related Topics
Upload Cisco Finesse Certificate to Cisco MediaSense Server, on page 94

MediaSense 11.5(1) Upgrade Consideration for Cisco Finesse Configuration

If you are upgrading from an earlier release to Release 11.5(1), you must change IP address or hostname of Finesse server to FQDN (fully qualified domain name).

Upload Cisco Finesse Certificate to Cisco MediaSense Server

To establish connection with Cisco Finesse securely, you must upload the Cisco Finesse tomcat certificate to Cisco MediaSense server.

Procedure

Step 1 Download the tomcat.pem certificate of Finesse host from the Unified CCX server.

a) Sign in to Cisco Unified Operating System Administration on the Unified CCX server.
b) Select Security > Certificate Management.
   The Certificate List screen appears.

c) Click Find.
   A list of certificates appears.

d) In the Common Name column, click the link of the Finesse host certificate. The Certificate type must be
tomcat and the Common Name must be the host name.
   The Certificate Details pop-up window appears

e) Click Download .pem File.
   The file gets saved on your system.

Step 2
Upload the certificate to the designated MediaSense server.

a) Sign in to Cisco Unified Operating System Administration on the primary MediaSense node.
b) Select Security > Certificate Management.
c) Click Upload Certificate/Certificate Chain.
d) From the Certificate Name drop-down list, select tomcat-trust.
e) Click Browse and navigate to the .pem file that you downloaded in the previous step.
f) Click Upload File.

Note
• If self-signed certificates are used on both MediaSense and Unified CCX, then you must upload
  MediaSense tomcat certificate to Tomcat trusted store of Unified CCX server also.
• After the certificate exchange, you must restart both MediaSense and Unified CCX servers.

MediaSense API User Configuration

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

---

**Caution**

If you modify the Unified Communications Manager 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 Communications Manager 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 userID (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 Communications Manager 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.

---

**Note**
Currently, an addition of up to 150 API users is supported for AXL authentication.

**Related Topics**
Unified Communications Manager Configuration, on page 90
Prune Policy Configuration

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, check **Automatically prune recordings after they are more than __days old, and when disk space is needed for new recordings** check box. When this check box is checked, 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 want to automatically 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 percent mark. When the disk usage crosses the 90 percent 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 want to use the preceding option (New Recording Priority mode) and, at the same time, you want 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 for those recordings that are created after the check box is unchecked. To remove unwanted data and free up disk space, use your client application. For more information, see the Cisco MediaSense Developer Guide.

---

**Note**

If this check box is unchecked, the Old Recording Retention mode is applicable only to those recordings that are created after the box is unchecked; it does not prevent prior recordings that were created previously from being pruned.

---

**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). For more information, see the System Thresholds section.

---

**Related Topics**

- Storage Threshold Values and Pruning Avoidance, on page 81

---

**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), check 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.
Caution

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 might temporarily impact system performance.

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

**Procedure**

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.

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

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.

**Incoming Call Configuration**

MediaSense enables you to assign one incoming call rule to each incoming dialed numbered address. Acting on an incoming call rule, each address can:

- Record audio of the incoming calls
- Record audio and video of the 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's audio streams. This system default rule appears in the first row in the list of incoming call rules on the **MediaSense Incoming Call Configuration** screen, regardless of how you sort the list.

If no incoming call rule has been assigned to an incoming address, MediaSense falls back on the system default rule when an incoming call arrives at that address.
On an upgrade from a previous release to Release 10.5 or later, if you are using Direct Inbound or Outbound Recording to record ad hoc videos from a phone, then you need to change the relevant Action to **Record Audio and Video** on the **MediaSense Incoming Call Configuration** screen, because on an upgrade the Action is set to **Record Audio Only** by default.

**Incoming Call Rules List**

The **MediaSense Incoming Call Configuration** screen displays a read-only list of the incoming call rules for each dialed number address that MediaSense might receive. Displayed in rows, you can view the address of an incoming call and the action that is an incoming call rule for that address. 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 address.

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 incoming address to use the editable system default rule.

**Add Incoming Call Rule**

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

**Procedure**

1. **Step 1** From the **Administration** menu, select **Incoming Call Rule Configuration**.
2. **Step 2** On the **Incoming Call Rule Configuration** toolbar, click **Add**.
3. **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:**

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 `5551212`.

4. **Step 4** From the **Action** drop-down list, select an incoming call rule. Possible values include Play Continuously, Play Once, Record Audio, Record Audio and Video, or Reject.
5. **Step 5** If the **Action** selected is Play Continuously or Play Once, then select a media file to play from the **Media File** drop-down list.
6. **Step 6** 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

1. **From the Administration menu, select Incoming Call Rule Configuration.**
2. **At the bottom of the Incoming Call Rule Configuration window, go to the Incoming Call Rules list and select the radio button for the call rule that you want to edit.**
3. **On the Incoming Call Rule Configuration toolbar, click Edit.**
4. **(Optional) In the Edit Incoming Call Rule window, 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.

5. **(Optional) In the Edit Incoming Call Rule window, go to the Action drop-down list and select a different incoming call rule for the endpoint.**
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.**
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 address to which you have not assigned another incoming call rule.

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

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

### Procedure

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

1. From the Administration menu, select Incoming Call Rule Configuration.
2. From the Incoming Call Rules list, select the radio button for the Incoming Call Rule that you want to delete.
3. Click Delete.
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 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. (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. You can upload the same media file again. 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 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 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 that 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.
• Entire MP4 file size must not exceed 2 GB.

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 is not 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**.

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**.

---

## Playlist Manager

Using the **Playlist Manager** window, you can add or manage a playlist of audio files to be played back when a caller waits for a call center agent to be available. The playlist contains uploaded media files that are played sequentially. Media is streamed over RTP under RTSP signaling control.

### Add a Playlist

Using the **Add Playlist** window, you can add a new playlist.

To add a new playlist, perform the following steps.

### Procedure

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

The **Media File Management** window appears.

**Step 2** Click the **Playlist Manager** button.

The **Playlist Manager** window appears.

**Step 3** Click the **Add** button.

The **Add Playlist** window appears.

**Step 4** In the **Playlist Name** text box, enter the name of the playlist and click the **Save** button.

The following message appears:
Successfully saved Playlist Name.

Limitations to a Playlist

Consider the following limitations while adding a playlist.

• Uploaded media files should be both audio and video.
• Playlist name should be a maximum of 20 alphanumeric characters.
• Maximum number of playlists allowed at a time is 10.
• Single playlist can have a maximum of 10 uploaded media files.
• Duration of uploaded media files should be less than 1 minute.
• An uploaded media file cannot be repeated in the same playlist.
• Only playlist URL with PCMU codec appears on the Playlist Manager window.
• An uploaded media file should not be deleted if already added in the playlist.

Manage a Playlist

After creating a new playlist, you can add media files to the playlist. You can select the media files from the Available Media Files list box. The selected media files appear in the Selected Media Files list box. The available media files must be in the Ready state to be played back.

Note

Save the changes made to the playlist before you perform another operation on the Playlist Manager window. Otherwise, the changes are not saved.

To manage a playlist, perform the following steps.

Procedure

Step 1
From the Administration menu, choose Media File Management.
The Media File Management window appears.

Step 2
Click the Playlist Manager button.
The Playlist Manager window appears.

Step 3
From the Select a Playlist drop-down list, choose the playlist to which you want to add or remove a media file.
The RTSP URL for the selected playlist appears in the RTSP Playback URL (PCMU) text box.
For example: URL for playlist "sample7": rtsp://<SERVER-IP>:8550/playlist/sample7.2
where Server-IP is the IP address of the MediaSense server.
Step 4  Perform the following steps:

- To add a media file, select the media file (if more than one, use the Ctrl key) from the Available Media Files list box and click the right arrow button.
  The selected media file appears in the playlist list box on the right-hand side.

- To remove a media file, select the media file (if more than one, use the Ctrl key) from the playlist list box on the right-hand side and click the left arrow button.
  The selected media file is removed from the playlist list box and appears in the Available Media Files list box.

Note You can change the sequence of the media files in the playlist list box by clicking the up or down arrow.

Step 5  Click Save.

The following message appears.

Successfully saved Playlist Name.

Archival

MediaSense can store various types of recordings like audio, video, and video greetings. However, the disk space on MediaSense cluster is limited. In case you want to save the recordings for an extended set of time, MediaSense has a feature called Archival. Using this feature, the specified recordings are automatically copied to an offline location in accordance with the archive configuration settings done in the MediaSense Archive Configuration screen.

MediaSense supports uploading a recording session to an archive server, and searching and downloading the session from the archive server. The archive server is provided by the user.

- Pre-requisites to archive a recording session:
  - Archive server should support SFTP.
  - User account with access to write to the server using SFTP.

  Note The SFTP server is Linux-based, which is required to search the archived recordings using the grep command.

- Pre-requisites to search and retrieve sessions:
  - Archive server should support SSH protocol.
  - Usage of Unix grep command.
  - User account with access to read from the server.
  - Only BASH shell should be used on the Linux-based SFTP server.
Run the command `echo $0` on your SFTP server to check which shell is being used. For BASH shell the output should be `-bash`.

To change the shell to `bash`, perform the following steps:

1. Enter `chsh -s /bin/bash`. 
2. Enter `exit` to log out of the SSH session.
3. Log in again and enter `echo $0`.

Verify the output is `-bash`.

Once a recording session is sent to the archive server, the user is responsible for all user access security, disk space management, retention and deletion policies.

The user account and password credentials can be same for both SFTP connection as well as SSH connection.

Note

E.164 phone numbers cannot be searched as a participant on MediaSense Search and Play on the 'Archive Calls' tab due to the '+' in the phone numbers. They can be searched via session ID or can be found manually on the SFTP server where the recording is archived.

To set the archive configuration, perform the following steps:

**Procedure**

**Step 1**
From the MediaSense Administration menu bar, click Archive Configuration. The MediaSense Archive Configuration window appears.

**Step 2**
In the MediaSense Archive Configuration window, check one or more of the following check boxes.

- Automatically Archive MediaSense Audio Recordings to automatically archive audio recordings.
- Automatically Archive MediaSense Video Recordings to automatically archive video recordings.
- Automatically Archive Video Greetings Recordings to automatically archive video greeting's recordings.

**Step 3**
Enter the time in the 12-hour format in the Start Archive at text box at which the archiving will start automatically. By default, the value is 01:00AM. Each day at the specified time, MediaSense computes the list of sessions to be archived, and starts the archiving process. It continues until the entire list of recordings has been completed.

**Step 4**
Enter the age (in days) of the recordings in the Archive Recording Older than text box after which the recordings are to be archived automatically. The days entered should be equal to or greater than 1. By default, the value is 7. If you have automatic pruning enabled, be sure to set this to a number less than the pruning retention period.
Step 5  
In the SFTP Location Configuration section, enter the values in the following mandatory fields.

a) Enter the domain name or IP of the server to which the archived recordings are to be stored in the Server Name (IP or FQDN) text box. By default, the value is sftphost.

b) Enter the absolute/full path to store archived recordings on the server in the Path Name text box. By default, the path is /.

c) Enter the user ID to log in to the server in the User Name text box. By default, the ID is sftpuser.

d) Enter the password for user authentication in the Password text box. By default, the password is sftppassword.

Step 6  
Click Test SFTP to authenticate the SFTP connection and credentials.

Note  
Please verify that the Path Name entered is correct and valid as Incorrect path name information also gets saved without any error messages.

Note  
In case you enter invalid/incorrect credentials or the SSH protocol fails to establish between the MediaSense and SFTP servers, this message appears in the window.

A General Error occurred. Contact your Administrator for more details.

The SFTP server might not agree with the MediaSense server on a key exchange algorithm, a message authentication code (MAC) algorithm, or a cipher for encrypting traffic.

To avoid the conflict, make sure the SFTP server negotiates with the Mediasense server on

- One of the following key exchange algorithms:
  diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1

- One of the following ciphers:
  aes128-cbc, 3des-cbc, blowfish-cbc, aes192-cbc, aes256-cbc

- One of the following MAC algorithms:
  hmac-md5,hmac-sha1, hmac-sha2-256,hmac-sha1-96, hmac-md5-96

Step 7  
In the Additional Configuration section, enter the number of simultaneous connections possible with the SFTP server in the Simultaneous Connections (For the MediaSense Cluster) text box. The value should be equal to or greater than 1, but should not be more than the number of nodes in a MediaSense cluster. By default, the value is set to 1.

Step 8  
Check the Enable Search on Archived Recordings check box to enable search of archived recordings in MediaSense Search and Play.

For more information, see the Search For, Play, or Downloaded a Recorded Call section.

The fields in the SSH Configuration section are enabled.

Step 9  
In the SSH Configuration section, check the Use SFTP username and password check box to use the same user name and password credentials entered for SFTP connection in the User name and Password text boxes, respectively.

Note  
In case the Use SFTP username and password check box is unchecked, the User name and Password text boxes are enabled and you can edit the displayed credentials.

Step 10  
Click the Test SSH text box to authenticate the SSH connection and the following actions:

- Ability to perform SSH on the specified server using the given credentials.
• Existence of the specified path name on the server.
• Read access to the user for the specified path.
• Ability to run the `grep` command on the specified server.

On successful authentication, this message appears in the window.

**Connection successful.**

**Step 11**

Click **Save** to save the archive configuration.

This message appears in the window.

**Successfully updated Archive Configuration data.**

**Note** You can reset all the values to default or last saved, by clicking the **Reset** button.

---

**Related Topics**

[Search For, Play, or Download a Recorded Call](#), on page 17

---

**Search and Play Configuration**

Using **Search and Play Configuration** screen, you can configure the following settings to customize various services in **MediaSense Search and Play**.

• Enable or disable the usage of In-browser player to play back a recording.

• Enable or disable the delete functionality.

• Enable or disable the appearance of Unified Communications Manager line name display in the search results.

• Restrict Finesse supervisors to access their teams’ recordings only.

• Select or deselect the parameters to appear as part of agent information in the search results.

The configured settings appear on both standalone MediaSense Search and Play and Finesse Search and Play gadget.

**Procedure**

**Step 1**

To configure the settings, perform one or more of the following actions:

• Check the **Enable In-browser Player** check box to activate in-browser player in **MediaSense Search and Play**.

  In **MediaSense Search and Play**, the in-browser player appears at the bottom of the selected audio recording showing the progress of the playback.

• Check the **Enable Delete Functionality** check box to activate the Delete icon in **MediaSense Search and Play**.

  In **MediaSense Search and Play**, the **Delete** icon is enabled.
• Check the **Show Line Display Name** check box to display Unified Communications Manager Line Name in the agent information.

In **MediaSense Search and Play**, Unified Communications Manager Line Name appears as part of agent information.

• Check the **Restrict Finesse Supervisors to their respective team's recordings only** check box to restrict Finesse supervisors to access recordings of their respective teams only. For more information, see Finesse Role-Based Access.

• In the **Agent Search and Display Options** section, select the parameters from the **Available Fields** list box that you want to display as part of agent information in MediaSense Search and Play. The available parameters are Login ID, Login Name, Last Name, First Name, Team ID, and Team Name.

The selected parameters appear as part of agent information in MediaSense Search and Play.

**Note** By default, all the check boxes are unchecked.

**Step 2**
Click **Save**.

The system displays the following message.

Successfully saved MediaSense Search and Play Configuration data.

---

**What to do next**

Next time a user signs in to **MediaSense Search and Play**, the new settings are effective. Users who are already logged in to **MediaSense Search and Play** will not view the result of the new settings until the next time they sign in.

**Related Topics**
- Finesse Role-Based Access, on page 25
- Search For, Play, or Download a Recorded Call, on page 17
- In-Browser Playback, on page 21

---

### MediaSense Administration System

Using MediaSense Administration System menu option, you can add a new server and manage media partitions.

### MediaSense Server Configuration

**Procedure**

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

**Step 2**
In the **MediaSense Server Configuration** window, click **Add MediaSense Server**.

The **Add MediaSense Server** window in the primary node opens.
Step 3  If your installation uses DNS, enter FQDN 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.

Note  It is mandatory to add secondary or expansion servers to MediaSense using FQDN only to seamlessly run features like in-browser playback.

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.

MediaSense displays a confirmation message near the top of the window. You see the configuration details of the server that you added in the MediaSense Server List. The server type is UNKNOWN at this stage of the installation.

Media Partition Management

Use the Media Partition Management window to manage the media partitions used on the MediaSense node that you are currently logged in to. 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 window 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, add more disk drives to the host (using VMware). After the system recognizes the new disks, you can increase the size of both of these partitions in chunks of 1.9 TB 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 can be expanded up to 15 TB of recordings for live and completed incoming calls.
- The /uploadedMedia partition can be expanded 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 that were originally installed with MediaSense 9.0 or earlier 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 labeled as /uploadedMedia. Like fresh installations, this partition can be expanded 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. This media partition is present when you do an upgrade from Release 9.0 (1) to Release 9.1(1) or later. After the upgrade, the storage capacity of the partition /uploadedMedia is 100 percent full. Follow the instructions to add storage space to the partition to upload your first media file.

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.
A message appears stating 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.

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. If a MediaSende 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.

MediaSende Administration provides a cluster-wide property to enable or disable event forwarding between the primary and secondary servers in any MediaSende 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 MediaSende cluster, follow this procedure.

**Procedure**

**Step 1**
From MediaSende Administration, select **System > Event Management**.

The MediaSende 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).
Enable Event Forwarding
MediaSense Serviceability

The MediaSense Serviceability menu bar contains the following options:

- **Trace**—Configures log and trace settings for MediaSense components. After enabled, you can collect and view trace information using the Unified Real-Time Monitoring Tool (Unified RTMT) and Cisco Prime Collaboration Assurance.

- **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, select **Help > This Page**.

- To verify the version of the administration running on the server, select **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, select **Help > Cisco.com**.
  
  If you are connected to the external network, this link connects you to the home page for MediaSense documents.

- To view the latest version of the troubleshooting tips for this release, select **Help > Troubleshooting Tips**.

  If you are connected to the external network, this link connects you to the Troubleshooting page for MediaSense.
You will be logged out from the MediaSense Serviceability Administration interface if the session remains idle for 30 minutes.

Access MediaSense Serviceability

After you complete the initial configuration 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.

Trace Configuration

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 to obtain specific, detailed information about the system so that 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.

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.

Note

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

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 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. 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 shows 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) and Cisco Prime Collaboration Assurance. Trace and Log Central is the Unified Communications component which manages and provides access to trace files. When the services start up (during the initial configuration process), the trace and log files are visible in the RTMT Trace and Log Central section after you launch Unified RTMT.


Setup Trace File Information

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 MediaSenseserver 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 and Cisco Prime Collaboration Assurance.

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 webpage 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](#).

## 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 suspend the host resources agent.

**Related Topics**

[utils Commands](#), on page 142
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 `utilsservice` 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 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**

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

- In-progress recordings may fail to complete properly when outages occur in the media service, call control service or database service and end in an error state even after the service is reactivated. Recordings in all other states will be fine.

- 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.

---

**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 HTTP 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 Communications Manager 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. For more information, see the Unified Communications Manager documentation.
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 the Download the Unified RTMT Plug-In section.

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.

Related Topics

Download the Unified RTMT Plug-In, on page 126

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 plug-in 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.
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 and Cisco Prime Collaboration Assurance enable you to view the counter values.

For more information on Unified RTMT and Cisco Prime Collaboration Assurance, see the Cisco Unified Real-Time Monitoring Tool Administration Guide and Cisco Prime Collaboration Contact Center Assurance Guide, respectively.

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 preconfigured 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 and Cisco Prime Collaboration Assurance displays both preconfigured alerts and custom alerts in Alert Central. Unified RTMT and Cisco Prime Collaboration Assurance organizes the alerts under several
tabs including System, Custom, and MediaSense. Although the System tab and Custom tab are the same as those tabs available in Unified Communications Manager, 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.

System condition alerts and perfmon counter alerts for MediaSense are visible on a dashboard of Cisco Prime Collaboration Assurance.

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**

<table>
<thead>
<tr>
<th>Service</th>
<th>Alert Service</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tomcat (config service)</td>
<td>SC_ConfigLostContactWithDB</td>
<td>The configuration service lost contact with its database service.</td>
<td>Check the MediaSense database service. Restart it if necessary.</td>
</tr>
<tr>
<td></td>
<td>SC_ConfigurationOOS</td>
<td>The configuration service is out of service.</td>
<td>Check the MediaSense database service. Restart it if necessary.</td>
</tr>
<tr>
<td></td>
<td>SC_ConfigurationLostContactWithAXL</td>
<td>The configuration service lost contact with its Unified Communications Manager AXL server.</td>
<td>Check the Unified Communications Manager AXL configuration. Modify or restart it if necessary.</td>
</tr>
<tr>
<td>Service</td>
<td>Alert</td>
<td>Description</td>
<td>Recommended Action</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MediaSense call control service</td>
<td>SC_RecordingLatencyWarning</td>
<td>Recording start latency exceeds warning threshold.</td>
<td>Check the media server. Restart it if necessary.</td>
</tr>
<tr>
<td></td>
<td>SC_CallControlOOS</td>
<td>Call control service is out of service.</td>
<td>Check the call control server. Restart it if necessary.</td>
</tr>
<tr>
<td></td>
<td>SC_CallControlLostContact WithAPI</td>
<td>Call control service lost contact with API Service.</td>
<td>Check the API server. Restart it if necessary.</td>
</tr>
<tr>
<td></td>
<td>SC_CallControlLostContact WithMedia</td>
<td>Call control service lost contact with media Service.</td>
<td>Check the Media server. Restart if necessary.</td>
</tr>
<tr>
<td></td>
<td>SC_CallControlLoadCritical</td>
<td>Call load exceeds critical threshold.</td>
<td>Reduce the load by decreasing the number of phones that are configured for recording in a given cluster or install an additional MediaSense server.</td>
</tr>
<tr>
<td></td>
<td>PC_CallControlMaximumHeap Memory ThresholdReached</td>
<td>Safeguards the MediaSense system from running out of memory. If this counter crosses the 128 MB memory threshold, the system triggers an alert.</td>
<td>Reduce the load by decreasing the number of phones that are configured for recording in a given cluster or install an additional MediaSense server.</td>
</tr>
<tr>
<td>Service</td>
<td>Alert</td>
<td>Description</td>
<td>Recommended Action</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tomcat API service</td>
<td>SC_APILostContactWithDatabase</td>
<td>API Service lost contact with its database service.</td>
<td>Check the MediaSense database service. Restart it if necessary.</td>
</tr>
<tr>
<td></td>
<td>SC_APIServiceOOS</td>
<td>API Service is out of service.</td>
<td>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).</td>
</tr>
<tr>
<td>MediaSense system service</td>
<td>SC_SystemServiceOOS</td>
<td>The system service is out of service.</td>
<td>Check system service. Restart it if necessary.</td>
</tr>
<tr>
<td>MediaSense database service</td>
<td>SC_DatabaseServiceOOS</td>
<td>database service is out of service.</td>
<td>Check the database service. Restart it if necessary.</td>
</tr>
<tr>
<td>MediaSense storage management</td>
<td>SC_DiskSpaceWarning</td>
<td>Available media storage level is low.</td>
<td>Consider deleting old recordings.</td>
</tr>
<tr>
<td></td>
<td>SC_DiskSpaceCritical</td>
<td>Available media storage level is critical. The system may fail to process new requests.</td>
<td>Delete old recordings to free up storage space.</td>
</tr>
<tr>
<td></td>
<td>SC_DiskSpaceEmergency</td>
<td>No media storage space is available. This server is not functional.</td>
<td>Delete old recordings to free up storage space.</td>
</tr>
<tr>
<td></td>
<td>SC_TotalUsedAudioPortsExceedsCapacity</td>
<td>Recording threshold has been reached and addition of more recordings will lead to a critical condition.</td>
<td>Add more recording capacity or reduce the recording load.</td>
</tr>
</tbody>
</table>
AMC Service and Unified Communications Manager 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 Communications Manager 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.

⚠️ Caution ⚠️

If for any reason the primary MediaSense server shuts down or is in a failed state, 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 💡

Navigate to Unified Communications Manager Administration (in the primary Cisco MediaSense server). Choose System > Service Parameters, then select the secondary MediaSense server from the drop-down list, and 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 Communications Manager 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.
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 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.

<table>
<thead>
<tr>
<th>MediaSense Service or Agent Name</th>
<th>Remote Browse Folder Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call control service</td>
<td>callcontrol</td>
</tr>
<tr>
<td>Media service</td>
<td>media</td>
</tr>
<tr>
<td>API service</td>
<td>ora</td>
</tr>
<tr>
<td>Configuration service</td>
<td>oraconfiguration</td>
</tr>
<tr>
<td>Database service</td>
<td>oradb</td>
</tr>
<tr>
<td>SM agent</td>
<td>storagemanagementagent</td>
</tr>
<tr>
<td>MediaSense administration</td>
<td>oraadmin</td>
</tr>
<tr>
<td>Serviceability administration</td>
<td>oraservice</td>
</tr>
<tr>
<td>System service</td>
<td>systemservice</td>
</tr>
<tr>
<td>Perfmon agent</td>
<td>perfmonagent</td>
</tr>
</tbody>
</table>
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 and Cisco Prime Collaboration Assurance. You can use Unified RTMT and Cisco Prime Collaboration Assurance 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.

<table>
<thead>
<tr>
<th>Counter Class and Name</th>
<th>Counter Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class: MediaSense Call Control Service</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Recording Sessions Counters</strong></td>
<td></td>
</tr>
<tr>
<td>Heap memory usage</td>
<td>Sends an alert when its value exceeds 128 MB of memory (to help keep MediaSense from running out of memory).</td>
</tr>
<tr>
<td>Number of active sessions</td>
<td>The number of active recording sessions.</td>
</tr>
<tr>
<td>Number of recorded sessions without errors</td>
<td>The number of recorded sessions completed without errors.</td>
</tr>
<tr>
<td>Number of recorded sessions with errors</td>
<td>The number of recorded sessions completed with errors.</td>
</tr>
<tr>
<td><strong>Recording Setup Time</strong></td>
<td></td>
</tr>
<tr>
<td>Mean setup delay</td>
<td>The average delay (in milliseconds) between the initial receipt of the SIP Invite from Unified Communications Manager and the SIP response to the Unified Communications Manager rolling window time.</td>
</tr>
<tr>
<td>Max setup delay</td>
<td>The maximum delay (in milliseconds) between the initial receipt of the SIP Invite from Unified Communications Manager and the SIP response to the Unified Communications Manager rolling window time.</td>
</tr>
<tr>
<td>Counter Class and Name</td>
<td>Counter Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>SIP-S Counters</strong></td>
<td></td>
</tr>
<tr>
<td>Total SIP-S calls</td>
<td>The number of successful (closed and completed) SIP-S calls.</td>
</tr>
<tr>
<td>Active SIP-S calls</td>
<td>The number of currently active SIP-S calls.</td>
</tr>
<tr>
<td>Failed SIP-S calls</td>
<td>The number of erroneous SIP-S calls.</td>
</tr>
<tr>
<td><strong>SRTP Counters</strong></td>
<td></td>
</tr>
<tr>
<td>Number of completed SRTP calls</td>
<td>The number of successful SRTP calls.</td>
</tr>
<tr>
<td>Number of active SRTP calls</td>
<td>The number of currently active SRTP calls, with or without errors.</td>
</tr>
<tr>
<td>Number of failed SRTP calls</td>
<td>The number of failed SRTP calls.</td>
</tr>
<tr>
<td><strong>Stream Dialog API (used by Video Greeting in Unity Connection)</strong></td>
<td></td>
</tr>
<tr>
<td>Started dialogs</td>
<td>The total number of stream dialogs started.</td>
</tr>
<tr>
<td>Start record API requests</td>
<td>The total number of successfully started stream dialog start recording requests.</td>
</tr>
<tr>
<td>Start playback API requests</td>
<td>The total number of successfully started stream dialog start playback requests.</td>
</tr>
<tr>
<td>Rejected dialogs due to busy</td>
<td>The total number of stream dialog start requests that returned BUSY.</td>
</tr>
<tr>
<td>Mean start record time</td>
<td>The average amount of time (in milliseconds) taken to successfully start a recording operation.</td>
</tr>
<tr>
<td>Mean start playback time</td>
<td>The average amount of time (in milliseconds) taken to successfully start a play operation.</td>
</tr>
<tr>
<td>Mean dialog time</td>
<td>The average amount of time (in milliseconds) a stream dialog was active.</td>
</tr>
<tr>
<td>Max start record time</td>
<td>The maximum amount of time (in milliseconds) taken to successfully start a recording operation.</td>
</tr>
<tr>
<td>Max start playback time</td>
<td>The maximum amount of time (in milliseconds) taken to successfully start a play operation.</td>
</tr>
<tr>
<td>Max dialog time</td>
<td>The maximum amount of time (in milliseconds) a stream dialog was active.</td>
</tr>
<tr>
<td>Completed dialogs</td>
<td>The total number of stream dialogs completed.</td>
</tr>
<tr>
<td>Counter Class and Name</td>
<td>Counter Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Average active dialogs on busy</td>
<td>The average number of stream dialogs (rounded down to nearest integer) that were active when a stream dialog start request returned BUSY.</td>
</tr>
<tr>
<td><strong>Class: MediaSense Media Service</strong></td>
<td></td>
</tr>
<tr>
<td>Number of active playbacks</td>
<td>The number of outgoing RTSP sessions.</td>
</tr>
<tr>
<td>Number of live monitored calls</td>
<td>The number of ports used for live-monitored calls. One live-monitored call uses two ports in most cases.</td>
</tr>
<tr>
<td><strong>Class: MediaSense Configuration Service</strong></td>
<td></td>
</tr>
<tr>
<td>Authentication request processing: average latency</td>
<td>The average latency for processing an authentication request.</td>
</tr>
<tr>
<td>Authentication request processing: max latency</td>
<td>The maximum latency for processing an authentication request.</td>
</tr>
<tr>
<td>Total requests</td>
<td>For Cisco use only.</td>
</tr>
<tr>
<td>Total failures</td>
<td>The total number of request failures encountered by the MediaSense configuration service.</td>
</tr>
<tr>
<td><strong>Class: MediaSense API Service</strong></td>
<td></td>
</tr>
<tr>
<td>Mean query response time</td>
<td>The average query response time in the last hour.</td>
</tr>
<tr>
<td>Max query response time</td>
<td>The maximum query response time in the last hour.</td>
</tr>
<tr>
<td>Total number of responses</td>
<td>The total number of successful and unsuccessful responses.</td>
</tr>
<tr>
<td>Total number of requests</td>
<td>The total number of requests received and serviced by the API Service.</td>
</tr>
<tr>
<td>Avg time per request</td>
<td>The average time for each request received and serviced by the Call Control Service in the last hour.</td>
</tr>
<tr>
<td>Max time per request</td>
<td>The maximum time for each request received and serviced by the Call Control Service in the last hour.</td>
</tr>
<tr>
<td>Max number of concurrent requests</td>
<td>The maximum number of concurrent requests received and serviced by the Call Control Service in the last hour.</td>
</tr>
<tr>
<td>Total number of concurrent requests in progress</td>
<td>The total number of concurrent requests in progress in the last hour.</td>
</tr>
<tr>
<td>Total number of agent logins</td>
<td>The total number of agent login events since the service started on a MediaSense node.</td>
</tr>
<tr>
<td>Total number of active logged-in agents</td>
<td>The total number of active agents currently logged in since the service started on a MediaSense node.</td>
</tr>
<tr>
<td>Counter Class and Name</td>
<td>Counter Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Total number of agent logouts</td>
<td>The total number of successful agent logouts from MediaSense through Finesse gadget.</td>
</tr>
<tr>
<td>Total number of sessions archived</td>
<td>The total number of sessions archived successfully since the API Service startup. Resets to zero upon service restart.</td>
</tr>
<tr>
<td>Number of sessions currently being archived</td>
<td>The number of sessions that are either currently being converted, currently being transferred, or converted and waiting to be transferred. This is a measure of archiving activity taking place in parallel, cluster wide.</td>
</tr>
<tr>
<td>Number of sessions to be processed for archival</td>
<td>The total number of sessions selected for archiving in the current scheduled archive window. This counter is populated once the scheduled window starts, and reduces by one each time a session is processed, whether successfully or unsuccessfully.</td>
</tr>
<tr>
<td>Number of sessions overdue for archival</td>
<td>The total number of sessions which failed to archive from previously scheduled archive windows, due to either failures or inadequate archiving capacity for the number of sessions selected. This counter is populated only at the beginning of each scheduled archive window and reduces by one each time a session is processed, whether successfully or unsuccessfully.</td>
</tr>
<tr>
<td>Number of sessions that failed to archive</td>
<td>The number of sessions which failed to archive due to errors during conversion or transfer in the current or most recent scheduled archive window.</td>
</tr>
</tbody>
</table>

**Class: MediaSense Storage Management Agent**

<table>
<thead>
<tr>
<th>Counter Class and Name</th>
<th>Counter Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common partition usage</td>
<td>The percentage of common partition disk usage.</td>
</tr>
<tr>
<td>Media # partition usage</td>
<td>The percentage of disk usage of each media partition.</td>
</tr>
<tr>
<td>Audio recording ports in use</td>
<td>The number of audio ports currently in use for recording.</td>
</tr>
<tr>
<td>Video recording ports in use</td>
<td>The number of video ports currently in use for recording.</td>
</tr>
<tr>
<td>Available audio ports</td>
<td>The number of audio ports available.</td>
</tr>
<tr>
<td>Available video ports</td>
<td>The number of video ports available.</td>
</tr>
<tr>
<td>Total audio ports in use</td>
<td>The number of audio ports currently in use.</td>
</tr>
<tr>
<td>Total video ports in use</td>
<td>The number of video ports currently in use.</td>
</tr>
<tr>
<td>Total RTSP playback requests</td>
<td>The number of RTSP playback requests.</td>
</tr>
<tr>
<td>Total RTSP playback requests last 5 min.</td>
<td>The number of RTSP playback requests in the last 5 minutes.</td>
</tr>
<tr>
<td>Rejected RTSP playback requests</td>
<td>The number of rejected RTSP playback requests</td>
</tr>
<tr>
<td><strong>Counter Class and Name</strong></td>
<td><strong>Counter Description</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Rejected RTSP playback requests last 5 min.</td>
<td>The number of rejected RTSP playback requests in the last 5 minutes.</td>
</tr>
<tr>
<td>Total RTSP monitoring requests</td>
<td>The number of RTSP monitoring requests</td>
</tr>
<tr>
<td>Total RTSP monitoring requests last 5 min.</td>
<td>The number of RTSP monitoring requests in the last 5 minutes.</td>
</tr>
<tr>
<td>Rejected RTSP monitoring requests</td>
<td>The number of rejected RTSP monitoring requests.</td>
</tr>
<tr>
<td>Rejected RTSP monitoring requests last 5 min.</td>
<td>The number of rejected RTSP monitoring requests in the last 5 minutes.</td>
</tr>
<tr>
<td>Total raw download requests</td>
<td>The number of raw download requests</td>
</tr>
<tr>
<td>Total raw download requests last 5 min.</td>
<td>The number of raw download requests in the last in 5 minutes.</td>
</tr>
<tr>
<td>Rejected raw download requests</td>
<td>The number of rejected raw download requests.</td>
</tr>
<tr>
<td>Rejected raw download requests last 5 min.</td>
<td>The number of rejected raw download requests in the last 5 minutes.</td>
</tr>
<tr>
<td>Total convert requests</td>
<td>The number of convert requests.</td>
</tr>
<tr>
<td>Total convert requests last 5 min.</td>
<td>The number of convert requests in the last 5 minutes.</td>
</tr>
<tr>
<td>Rejected convert requests</td>
<td>The number of rejected convert requests.</td>
</tr>
<tr>
<td>Rejected convert requests last 5 min.</td>
<td>The number of rejected convert requests in the last 5 minutes.</td>
</tr>
<tr>
<td>Failed Convert Requests</td>
<td>The number of failed conversion attempts on a node since Storage Management Agent service startup. Resets to zero upon service restart.</td>
</tr>
<tr>
<td>Total Transfer Requests</td>
<td>The number of file transfer requests on a node since Storage Management Agent service startup. Resets to zero upon service restart.</td>
</tr>
<tr>
<td>Failed Transfer Requests</td>
<td>The number of failed file transfer attempts on a node since Storage Management Agent service startup. Resets to zero upon service restart.</td>
</tr>
<tr>
<td>Consecutive Failed Convert Requests</td>
<td>The number of consecutive failed conversion attempts on a node. Resets to zero after any successful conversion.</td>
</tr>
<tr>
<td>Consecutive Failed Transfer Requests</td>
<td>The number of consecutive failed file transfer attempts on a node. Resets to zero after any successful file transfer.</td>
</tr>
</tbody>
</table>

**Class: MediaSense Database Service**

This class has no perfmon counters.
Cisco Prime Collaboration Assurance Administration

To configure Cisco Prime Collaboration Assurance with MediaSense, perform the following steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>In Cisco Prime Collaboration Assurance window, choose Operate &gt; Device Work Center. The Device Work Center window appears.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the Device Work Center window, click Manage Credentials.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the Discover Devices dialog box, perform the following actions:</td>
</tr>
<tr>
<td>1.</td>
<td>In the Profile Name text box, enter the profile name.</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional) From the Device Type drop-down list, choose the type of device.</td>
</tr>
<tr>
<td>3.</td>
<td>From the IP Version drop-down list, choose the IP version.</td>
</tr>
<tr>
<td>4.</td>
<td>In the IP Address Pattern text box, enter the IP address.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>In the General SNMP Options section, perform the following actions (optional):</td>
</tr>
<tr>
<td>1.</td>
<td>From the SNMP Timeout drop-down list, choose the number of seconds after which SNMP times out.</td>
</tr>
<tr>
<td>2.</td>
<td>From the SNMP Retries drop-down list, choose the number of SNMP retries allowed.</td>
</tr>
<tr>
<td>3.</td>
<td>From the SNMP Version drop-down list, choose the version of SNMP as 2c.</td>
</tr>
</tbody>
</table>

On selecting the SNMP version, you need to add the SNMP version details.

| Step 5 | In the SNMP V2 section, perform the following actions: |
| 1. | In the SNMP Read Community String text box, enter the community string. |
| 2. | In the Re-enter SNMP Read Community String text box, reenter the community string. |
| 3. | (Optional) In the SNMP Write Community String text box, enter the community string. |
4. (Optional) In the Re-enter SNMP Write Community String text box, reenter the community string.

Note For more information, refer Simple Network Management Protocol.

Step 6 In the HTTP(s) and JTAPI sections, enter the user name and password of Cisco MediaSense Unified Serviceability.

Step 7 Click Save.

Step 8 In the Discover Devices screen, click Device Discovery.

a) In the IP Address text box, enter the MediaSense IP address that you want to configure.

b) In the Schedule section, click the Start Time radio button and specify the start time and click a Recurrence radio button to specify the recurrence.

Step 9 Click Schedule and Run Now.

A successfully scheduled job message appears.

Step 10 In the Device Work Center window, check the state and status of MediaSense IPs to be Managed and Discovered Successfully, respectively.

Step 11 For monitoring MediaSense, choose Home > UC Performance Monitor.

Step 12 From the Cluster or Device drop-down list, choose MediaSense > &lt;MediaSense server&gt;.

Step 13 From the Dashboard drop-down list, choose the dashboard you want to monitor.

Note You can also create custom dashboards based on the monitoring requirements. For more information, refer Cisco MediaSense dashboards.

---

**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.
Other Browser-Based Serviceability Tools

The information obtained from `show tech call_control_service detailed` and `utils media recording_sessions file filename` commands can also be obtained through a web browser using API user credentials. Both these serviceability tools are node-specific. You can put only one of the nodes into the `<hostname>` field of the URL, and you get information about the node only.

To generate an HTML file with a detailed list of the last 100 recording sessions processed by the MediaSense server, access the following URL.

https://<hostname>:8442/ora/service/sip/Sessions

`hostname` is the IP address of your MediaSense server.

The HTML file displays the following information:

- **Id** is the row number in the report.
- **Start** is the date and time at which the call started.
- **Duration** is the duration of the call.
- **Participant** is the participant identifier.
- **xRefci** is the reference call identifier for a particular media stream.
- **Type** is the category of the call whether audio or video for Built-in-Bridge recordings.
- **State** is the status of the call (in progress, closed, paused, and hold)
- **Name** is the session identifier.
- **Rtsp** is the real-time streaming protocol to play the recording. HTTP-BASIC credentials will be required.
- **Guid** is the global call identifier for Unified Border Element recordings.

To get information about the MediaSense call control service that runs on the system, access the following URL.


The HTML page provides information about the system memory, CPU usage, system details and conditions, initial configuration properties, recording sessions, recording setup time and other statistics, and Call Control Service configuration.
CHAPTER 6

MediaSense Command Line Interface

- Introduction, on page 141
- CLI Access, on page 141
- utils Commands, on page 142
- run Commands, on page 144
- set network Commands, on page 145
- show Commands, on page 148

Introduction

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.

---

Note

The disk size will be correctly shown for the first 5 disks, after which it will display the size as 0GB at the beginning of the Command Line Interface. This however has no overall functional impact.

In addition to the CLI commands listed in the Command Line Interface Guide for Cisco Unified Communications Solutions and this chapter, you can also enter the following commands:

- **help** displays the list of all supported commands. For example, to display help for a specific command, type `help utils service list` and press Enter.
- **quit** closes 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 enter 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
```
You can also view this information through a web browser. For details, see the Other Browser-Based Serviceability Tools section.

Related Topics
Other Browser-Based Serviceability Tools, on page 140

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 reboots when it enters maintenance mode. Any streaming activities end abruptly. Any active recordings end in a CLOSED_ERROR state. MediaSense reboots again when maintenance mode is disabled and it reenters 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 multiserver 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. Enter this command on the primary MediaSense server only. Entering this command on any other server results in an error.

Caution
This command may impact the synchronization of MediaSense services. Enter 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 enter this command. In each case, the CLI reports a success or error as applicable.

• With no arguments: If you enter 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. Enter 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 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. Enter 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

*** WARNING ***
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

---

**set useHostNameForMediaURL**

This command sets the media URLs (httpUrl, rtspUrl, mp4Url, wavUrl, and downloadUrl) to use the hostname, FQDN, or IP of a node, whichever is shown on the MediaSense Server Configuration window. The media URLs are used for MP4 or WAV download and playback of recording sessions on MediaSense Search and Play.

The values can be set to true or false.

- **true**—To set the media URLs to use the hostname, FQDN, or IP of the node, whichever is shown on the MediaSense Server Configuration window. Restart the MediaSense Configuration Service to activate this property.

- **false**—To set the media URLs to use only the IP address of the node.

Example:

```
admin:set useHostNameForMediaURL true
```

You will need to restart the Configuration Service to activate this property.

---

**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 status* 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 DBPub authenticated
2 10.10.10.93 mcs_vm93.cisco.com mcs_vm93 Secondary ora DBSub authenticated using TCP since Tue Aug 30 14:05:34 2011
3 10.10.10.100 mcs_vm100.cisco.com mcs_vm100 Expansion ora DBSub 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 enter 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`

---

**Note**

You can also get this information through a web browser. For details, see the *Other Browser-Based Serviceability Tools* section.

---

**Related Topics**

- *Other Browser-Based Serviceability Tools*, on page 140

---

**show useHostNameForMediaURL**

This command shows the status of the `useHostNameForMediaURL` property currently set on MediaSense Administration command prompt.

**Example:**

```
admin:show useHostNameForMediaURL

propertyname  sub.hostname.for.ip
propertyvalue  true
```
CHAPTER 7

MediaSense Terminology

- Playback, on page 151
- Blog Recording, on page 152
- Media Forking, on page 152
- Sessions and Recording Sessions, on page 152
- Glossary of Common Terms, on page 152

Playback

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. For more information about using the APIs, see the Cisco MediaSense Developer Guide.

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. For more information, see the Playing Back Recordings section of the Cisco MediaSense Developer Guide.
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**

Unified Border Element deployments do not support direct outbound recording.

Mid-call codec changes are not supported for direct inbound or direct outbound calls.

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 Communications Manager documentation](#).

Unified Border Element does not have a BIB because the call forking is performed within the Unified Border Element application and 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 Communications Manager. For more information about recording sessions, see the [Cisco Unified Communications Manager Features and Services Guide](#).

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 that is a phone number or extension for each device. The device ID is the unique identifier for each device and it corresponds directly to the name of the device (such as 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 of Common Terms

**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 the meta 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 rebooted 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 reboot 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 Communications Manager. For more information about its recording sessions, see the Cisco Unified Communications Manager Features and Services Guide.
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, start date, and track number. 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.