Cisco MediaSense Administration

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

Single sign-in

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

- Cisco MediaSense Administration
- Cisco MediaSense Serviceability Administration
- Cisco Unified Serviceability

Caution Cisco Unified OS Administration and Disaster Recovery System requires a separate (Unified CM) authentication procedure.

To access these applications from the Cisco MediaSense Administration, you must first select the required application from the Navigation drop-down list box and click **Go.**

Access Cisco MediaSense Administration

To access the Cisco MediaSense Administration, you need the Application Administrator User ID and case-sensitive password that were defined when you installed Cisco MediaSense. See 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://servername/oraadmin`.
The *servername* is the IP address of the server on which you installed Cisco MediaSense.

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

The Cisco 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 Cisco MediaSense version number, as well as trademark, copyright, and encryption information.

Administration navigation and menus

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

Navigation

After you log on, the main Cisco MediaSense Administration web page appears. The web page includes the drop-down list box in the upper right corner called Navigation. To access the applications in the drop-down list box, choose the required application and click **Go**.

The choices in the drop-down list box include the following Cisco MediaSense-related applications:

- **Cisco MediaSense Administration:** Use the Cisco MediaSense Administration to configure Unified CM, Cisco MediaSense users, prune policy, and other procedures described in this section.
- **Cisco MediaSense Serviceability Administration:** Takes you to the main Cisco MediaSense Serviceability web page that is used to configure trace files, and to enable and disable Cisco MediaSense services. See Serviceability Administration.
- You must be an end user on the configured Unified CM with Administrator capability in Cisco MediaSense to sign in to any of the Cisco MediaSense-related applications.

- **Cisco Unified OS Administration:** Takes you to main Cisco Unified OS Administration web page, so you can configure and administer the Cisco Unified Communications platform for Cisco MediaSense. Access the Unified OS Administration directly for more information.
- **Cisco Unified Serviceability:** Takes you to the main Cisco Unified Serviceability web page that is used to configure trace files and alarms and to enable and disable Cisco Unified Communications services.

The Cisco MediaSense Administration menu bar appears at the top of every web page in the Cisco MediaSense Administration web interface. You begin every Cisco MediaSense configuration and administration task by choosing a menu and submenu option from the menu bar.

Administration main menu

The Cisco MediaSense Administration menu bar contains the following menu options:

- **Administration**—Contains options for configuring new servers in the cluster, Unified CM information, and changing system parameters. For a description of all Administration menu options, see Access Cisco MediaSense Administration.
- **System**—Allows you to add a new server or view the disk usage information for each server in the Cisco MediaSense deployment.
- **Help**—Provides access to online help for Cisco MediaSense.

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

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

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

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

Field and parameter tool tips

All Cisco MediaSense Administration pages provide descriptive tool tips for each parameter and field. When you place your mouse over the required parameter and field, the tool tip information is briefly displayed for each parameter and field. Because the required information for each parameter and field are already provided within these tool tips, this document does not repeat that information.

Unified CM cluster configuration

The following information applies to a Unified CM cluster, assuming that the Unified CM administrator and Cisco MediaSense administrator are the same person, although they can also be two separate people.

Unified CM provisioning for Cisco MediaSense

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

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

Set up Call Control Service connection

The Call Control Service in Cisco MediaSense is referred to as a SIP Trunk in Unified CM UI and documentation. In the Unified CM Administration, you must configure the SIP Trunk, Route Group, Route List, and Recording Profile to enable the Call Control Service in the Cisco MediaSense Administration to communicate with the Unified CM Administration.

Note Be sure to configure Unified CM to use TCP transport for a SIP Trunk connection to Cisco MediaSense.

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

Even if already enabled, the Call Control Service will not be *In service* until you have configured the Call Control Service Provider.

To configure the SIP Trunk information in Unified CM, follow this procedure.

Procedure

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

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

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

Step 3 Select **Device** > **Trunk** in the Unified CM Administration.
Follow the procedure specified in your Unified CM Administration documentation to add a new SIP Trunk. Configure the Device name, select the Device Pool, assign SIP information, enter the destination (in this case, Cisco MediaSense) IP address and port (5060), select the SIP trunk security profiles and SIP profile (created in Step 2) and save this configuration.

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

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

Select all the Cisco MediaSense SIP trunks created in Step 3.

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

Step 6 Create a Route Pattern by selecting **Call Routing** > **Route/Hunt** > **Route Pattern** in the 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 the Unified CM Administration.
Follow the procedure specified in your Unified CM Administration documentation to add a new Recording Profile. Configure the Recording Profile name, and the Recording Destination Address (enter the Route Pattern number you configured in Step 6), and click **Save.**

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

a) Find the audio forking phone.
b) Find the Built In Bridge configuration for this device and change the setting to **ON.**
c) Access the Directory Number Configuration page for the line to be recorded.
d) Enable Recording by selecting **Automatic Call Recording Enabled** in the Recording Option drop-down list.
e) Select the Recording Profile created earlier in this procedure.

Step 9 To prevent Unified CM from sending Session Description Protocol (SDP) invitations, be sure to uncheck the Media Termination Point (MTP) Required field (or verify that it is already unchecked).

Disable iLBC and iSAC for recording device

Cisco MediaSense recording sessions using the following supported Codecs:

- Audio recordings: g.711 (aLaw or μ-Law), g.722, or g.729 (a/b) Codecs
- Video recordings: h.264 Codecs

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

Note This procedure provides steps for Unified CM Release 8.5. See the related Unified CM documentation for each corresponding release.

Procedure

Step 1 Select **System** > **Service parameters** in the Unified CM Administration.

Step 2 On the Service Parameter Configuration web page, select the required server and service (Cisco CallManager) from the **Select Server and Service** drop-down lists.

Step 3 Go to the Cluster-wide Parameters (Location and Region) section and locate the **iLBC Codec Enabled** parameter and the **iSAC Codec Enabled** parameter.

Step 4 Set the value for both of these parameters as *Enable for All Devices Except Recording-Enabled Devices* and save your configuration.

Unified CM user information and Cisco MediaSense setup

When you access the Cisco MediaSense Administration for the first time in a cluster, the system automatically initiates the cluster setup procedure that is described in the "Post-installation tasks" section of the *Cisco MediaSense Installation and Administration Guide*.

Select AXL service providers

During the Cisco MediaSense post-installation setup process, you may have provided the AXL information for the primary server. Based on the primary server information, the Cisco MediaSense Administration retrieves the list of other Unified CM servers in the cluster and displays them in the list of *available* Unified CM servers. You can select the required server (or servers) and change the Administrative XML Layer (AXL) user information. If you did not provide this information during the post-installation process or if you need to modify the AXL information, you can do so by following the procedure provided in this section.

Caution The AXL service must be enabled for the required Unified CM server (or servers) before the Cisco MediaSense Administration can access that server so you can update the AXL user information.

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

Procedure

Step 1 From the Cisco 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.

Caution The Unified CM username and password information are mandatory fields. The password cannot be updated on this page. You will need to change the password in the Unified CM administration. The Unified CM username and password information are mandatory fields. The password cannot be updated on this page. You will need to change the password in the Unified CM administration.

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

Step 4 Click the **Save** icon at the top of the Cisco Unified CM Configuration web page to save your changes. The Cisco 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 Cisco MediaSense installation process, you provided the information for the first Unified CM server. Based on the primary server information, Cisco MediaSense retrieves the list of other Unified CM servers in the cluster and displays them in the list of *available* Unified CM servers. You can select the required server so the Cisco MediaSense Call Control Service can determine the Unified CM server to which the outbound call must be sent. Outbound call refers to the call sent to one of the selected Unified CM servers by the Cisco MediaSense Call Control Service. If you select multiple Unified CM servers, you can ensure that the outbound call is placed even if one of the servers is not functional.

To modify the Call Control Service information for Cisco MediaSense, complete the following procedure.

Procedure

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

Step 2 In the Unified CM Configuration web page, go to the AXL Service Provider Configuration section to modify the AXL information using the following fields.

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

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

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

Replace Unified CM service providers

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

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

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

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

Procedure

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

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

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

Step 4 Click the **Save** icon at the top of the Add New AXL Service Provider web page to save your changes.

Note The initial list of selected AXL service providers on the Unified CM Configuration web page will be replaced with the selected Unified CM service provider.

The Cisco 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 Cisco MediaSense database.

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

Step 5 The list of Available Call Control Service Providers is also updated automatically for the newly selected service provider. Select and move the required Unified CM servers from the Available Call Control Service Provider list to the Selected Call Control Service Provider list using the right arrow.

Caution If you do not select the required Call Control Service Providers for the new Unified CM server, the Cisco MediaSense Call Control Service will be Out Of Service (OOS) and the outbound call recording will be disabled.

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

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

Cisco MediaSense setup with Cisco Unified Border Element

In Release 9.0(1), even with the Cisco Unified Border Element (CUBE) deployment model, Cisco MediaSense requires Unified CM authentication for all Cisco MediaSense users. All Unified CM User ID restrictions apply.

Manage Unified CM users

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

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

Cisco MediaSense provisioning for CUBE

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

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

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

- Select AXL service providers, on page 6
- Replace Unified CM service providers, on page 7
- Provision users for Cisco MediaSense deployment , on page 16

Note You do not need to configure Call Control service providers in Cisco MediaSense for any CUBE deployment.

CUBE and Cisco MediaSense setup

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

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

- CUBE Gateway accessibility, on page 10
- CUBE view configuration commands, on page 10
- Global-level interoperability and Cisco MediaSense setup, on page 11
- Dial-peer level setup, on page 12

CUBE Gateway accessibility

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

Table 1: CUBE Access Information

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

CUBE view configuration commands

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

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

Table 2: IOS Commands to View CUBE Configuration

Command	Description
`show running-config`	Displays the existing configuration for this CUBE gateway.
`show startup-config`	Displays the startup configuration for this CUBE gateway.

Command	Description
`show version`	Displays the IOS version being used in this CUBE gateway.
`show call active voice summary`	Displays the number of active SIP calls.

Global-level interoperability and Cisco MediaSense setup

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

Set up global level

Procedure

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

Step 2 Enter the global configuration mode.

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

Step 3 Enter VoIP voice-service configuration mode.

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

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

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

Step 5 Enable CUBE and CUBE Redundancy.

```
cube(config-voi-serv)#  allow-connections sip to sip
cube(config-voi-serv)#  mode border-element
```

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

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

a) Save your CUBE configuration.

```
cube# copy run start
```

b) Reboot CUBE.

```
cube# reload
```

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

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

Step 8 Exit the VoIP voice-service configuration mode.

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

Step 9 Create one voice codec class to include three codecs (G.711, G.729, G.722). These codecs will be used by the inbound dial-peer to specify the voice class.

```
cube(config)# voice class codec 1
cube(config)# codec preference 1 g711ulaw
cube(config)# codec preference 2 g729br8
cube(config)# codec preference 3 g722-64
```

Step 10 To simplify debugging, you must synchronize the local time in CUBE with the local time in Cisco MediaSense servers.
For example, if you specify the NTP server as 10.10.10.5, then use the following command in CUBE:

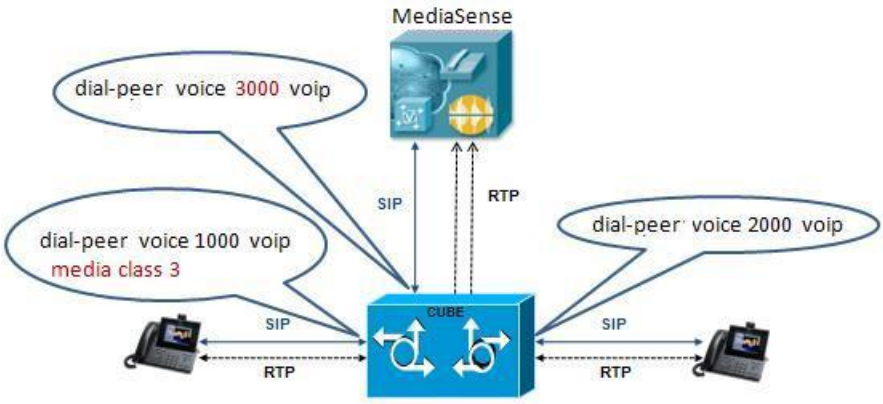
```
cube(config)#  ntp update-calendar
cube(config)#  sntp server 10.10.10.5
```

Dial-peer level setup

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

Each Cisco MediaSense deployment for CUBE contains three dial-peers:

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



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

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

Set up CUBE dial-peers for Cisco MediaSense deployments

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

Procedure

Step 1 Set up the inbound dial-peer.

a) Assign a unique name to the inbound dial-peer: dial-peer voice 1000 voip:

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

Places you in the dial-peer configuration mode to configure a VoIP dial-peer for 1000.

b) Specify the session protocol for this inbound dial-peer: session protocol sipv2.

```
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. (six digits, the first three digits are 123 and the last three digits are arbitrarily assigned by the system).

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

The string for the called-number must be 6 digits, with the first three being 123. The last three digits in this string are arbitrarily assigned by CUBE. This command associates the incoming call with a dial-peer.

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.

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

The tag used in this example is 1. This tag uniquely identifies this codec. Range is 1 to 10000.

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

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

f) Specify that everything that is going through the inbound dial-peer can be forked. Use the same number that you used to set up global forking (see Set up global level).

```
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.

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

Places you in the dial-peer configuration mode to configure a VoIP dial-peer for 2000.

b) Specify the session protocol for this outbound dial-peer: session protocol sipv2.

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

c) Specify the destination corresponding to the incoming called number.

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

d) When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to apply the class to individual dial-peers.

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

Use the same tag used for the inbound dial-peer.

e) If the call need not be recorded it needs to go to another destination instead of Cisco MediaSense. Specify the network-specific address for this destination.

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

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

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

Step 3 Configure the forking dial-peer.

a) Assign a unique name to the forking dial-peer.

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

Places you in the dial-peer configuration mode to configure a VoIP dial-peer for 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: session protocol sipv2.

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

c) Specify a fixed destination pattern with no wildcards. Calls recorded from this CUBE will appear to come from this extension.

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

d) When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to apply the class to individual dial-peers.

```
cube(config-dial-peer)# voice-class codec 1
```
Use the same tag used for the inbound dial-peer.

e) Provide the IP address of one of the Cisco MediaSense expansion servers, if available, as a destination for the CUBE traffic. Avoid using the primary or secondary Cisco MediaSense servers for this step (*if possible*) as this server must carry the CUBE load and you must avoid overloading the database server.

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

f) Set the session transport type (UDP or TCP) to communicate with Cisco MediaSense. The default is UDP.

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

The transport protocol specified with the session transport command, and the protocol specified with the transport command, must be identical.

g) Configure a heartbeat mechanism to monitor connectivity between endpoints.

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

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

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

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

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

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

j) Exit the configuration mode.

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

k) Save your CUBE configuration.

```
cube# copy run start
```

CUBE deployments log commands

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

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

Table 3: Useful Log Commands for CUBE Deployments

Command	Description
`service timestamp debug datetime msec localtime show-timezone`	Specifies the millisecond (msec) timestamp for various debug events.
`service timestamps log datetime msec localtime show-timezone`	Specifies the millisecond (msec) timestamp for various log events.
`localtime logging buffered 1000000`	Specifies the memory allocation for CUBE logins.
`no logging rate-limit`	Specifies that all log messages should be logged.
`no logging console`	Specifies that log messages should not be displayed on the console.

Provision users for Cisco MediaSense deployment

You can provision Unified CM end users as (Application Programming Interface (API) users in Cisco MediaSense deployments. This API access can be provided only by the Cisco MediaSense application administrator to the required Unified CM end users.

Cisco MediaSense API users

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

- Pause/resume, hold/resume, or conference/transfer a recording while in progress

- Control a recorded session
- Search and manage existing recordings
- Monitor a live session

Cisco MediaSense APIs provide an alternate to the functionality that is available through the Cisco MediaSense web interfaces. Using these APIs, API users can create customized client applications. Cisco MediaSense system integrators and developers who want to use Cisco MediaSense to integrate with other Unified Communications software or any third-party software applications need to have access to the Cisco MediaSense API. This API access can be provided only by the Cisco MediaSense administrator to the required Unified CM Users. See Unified CM user information and Cisco MediaSense setup, on page 6.

API user management

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

For more information see the following sections:

- API functionality overview: see Play back.
- About API users: see Cisco MediaSense API users, on page 16.
- API usage: see the *Developer Guide for Cisco MediaSense* at http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html.

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

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

Procedure

Step 1 Select **Administration** > **MediaSense User Configuration** from the Cisco MediaSense Administration. The MediaSense API User Configuration web page opens to display 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 of MediaSense API users, click **Manage MediaSense Users** .
The MediaSense API User Configuration web page opens to display the available Unified CM users in the Available Unified CM Users list and the configured API users in the MediaSense API Users list.

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

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

Step 4 Use the left and right arrows to make the required modifications to the MediaSense user list and click **Save**. The MediaSense API User Configuration web page 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 Cisco MediaSense User List page.

Storage Management Agent

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

Pruning options

Cisco MediaSense deployments provide pruning options to address varied deployment scenarios. In Cisco MediaSense Release 9.0(1), pruning options are specified in the **Administration** > **Prune Policy Configuration** page.

These pruning options allow you to enter the following modes:

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

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

- The age of the recording is equal to or greater than the retention age that you specify in the field for this option.

  For example, if you are within your disk usage percentage and if you automatically wish to delete all recordings older than 90 days, you must enter 90 in the *Automatically prune recordings after they are more than __days old, and when disk space is needed for new recordings* field. In this case, all recordings which are older than 90 days are automatically deleted. The range of values that can be specified for this option is 1 to 180 days. The default value is 60 days.

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

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

Note

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

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

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

- To have MediaSense remove the associated data automatically, select the *Automatically remove associated data and mp4 files* radio button.
- If you select the *Do not automatically remove associated data and mp4 files* radio button, the associated data will not be removed automatically. Instead, your client application must explicitly remove automatically pruned recordings, by way of the `getAllPrunedSessions` API and the `deleteSessions` API. When the `deleteSessions` API is executed, the metadata is *marked* as deleted, and the mp4 files are deleted. At midnight (local server time) daily, these database records are physically removed from the disk.

To place the priority on retaining older recordings (Old Recording Retention mode), uncheck the *Automatically prune recordings after they are more than __days old, and when disk space is needed for new recordings* check box. If this check box is unchecked, Cisco MediaSense does not automatically prune data. Instead, you must use your client application to remove unwanted data and free up disk space. See the *Developer Guide for Cisco MediaSense , Release 9.0(1)*) at http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html for more information.

Caution If you do not clean up unwanted data periodically, the Call Control Service rejects new calls and drop existing recordings at the emergency threshold level (ENTER_EMERGENCY_STORAGE_SPACE). See Storage threshold values and pruning avoidance, on page 20 for more details.

Set up pruning policy settings

Use the following information as a guide, if you want set up automatic pruning (New Recording Priority mode).

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

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

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

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

Procedure

Step 1 Select **Administration** > **Prune Policy Configuration** from the Cisco MediaSense Administration.
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 allowed range is from 1 to 180 days (the default is 60 days).

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

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

Storage threshold values and pruning avoidance

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

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

For more information about these options see Pruning options, on page 18.

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

Table 4: Storage Threshold Values

Threshold Storage	Percentage	Description
ENTER_LOW_STORAGE_SPACE	Recorded media crossed the 75% storage utilization mark.	First warning to indicate that the disk storage is running into low space condition.
EXIT_LOW_STORAGE_SPACE	Recorded media usage dropped below 70% utilization mark.	The disk storage is exiting the low storage space condition.
ENTER_CRITICAL_STORAGE_SPACE	Recorded media crossed the 90% local storage utilization mark.	Second warning. When entering this condition, action must be taken to guarantee future recording resources on this server. If operating in the Old Recording Retention mode (no automatic pruning), new recording sessions are not accepted when you reach this threshold. If operating in the New Recording Priority mode, older recordings are subject to automatic deletion (to make room for new recordings).
EXIT_CRITICAL_STORAGE_SPACE	Recorded media usage dropped below the 85% utilization mark.	The disk storage is exiting the critical storage space condition. At this point the local server is still considered to be low on resources. In the New Recording Priority Mode, the default pruning stops and only retention-based pruning is in effect.

Threshold Storage	Percentage	Description
ENTER_EMERGENCY_STORAGE_SPACE	Recorded media crossed the 99% storage utilization mark	Last warning. When the disk storage enters this condition, you must take action to guarantee future recording resources on this server. In addition to actions taken when in CRITICAL condition, all ongoing recordings are dropped and the node is considered out-of-service for recording purposes.
EXIT_EMERGENCY_STORAGE_SPACE -	Recorded media usage dropped below the 97% utilization mark.	The disk storage is exiting the emergency storage space condition. At this point, the local server is still considered to be low on resources and new recording sessions are still not accepted in the retention priority mode. In New Recording Priority mode, the server will process new recording requests.

See the *Developer Guide for Cisco MediaSense , Release 9.0(1)*:http://www.cisco.com/en/US/products/ps11389/products_programming_reference_guides_list.html for more details about the corresponding APIs, Events, and error code descriptions.

The following APIs and events correspond to this task:

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

System thresholds

The storage thresholds are monitored by the Storage Management Agent (SM Agent) on a per server basis. The thresholds are dedicated to the space used in 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 usage

To view and monitor the disk space usage in each server in the Cisco 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 usage information is not displayed. You may need to verify the state of your server to verify if it is reachable (using the `ping` command).

See Storage threshold values and pruning avoidance, on page 20 for more information about threshold value percentages.

Procedure

Step 1 From the Cisco 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 usage for the selected server in gigabytes (GB) or terabytes (TB) depending on the size of the disk drive. This page is read-only.

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

Storage usage information obtained using HTTP

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

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

The storage usage information is provided in an XML format.

- Example 1— Does not use any media disks:

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

- Example 2—Uses two media partitions:

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

 <partitions>
```

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

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

Storage usage information obtained by using Unified RTMT

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

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

Effective, Release 8.5(2), (Unified RTMT) displays all partitions in Cisco MediaSense and in the Unified Communications OS. Depending on the number of disks installed, the corresponding number of media partitions are visible in the Disk Usage window. If you do not install any media partitions, only Partition Usage (common media) is visible.

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

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

Event management

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

Enable event forwarding

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

However, the Cisco MediaSense Administration provides a cluster-wide property to enable/disable event forwarding between the primary and secondary servers in any Cisco MediaSense cluster. By default, forwarding is disabled in Cisco MediaSense deployments 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 Cisco MediaSense cluster, follow this procedure.

Procedure

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

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