Cisco 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.

New Features

IPv6

Cisco MediaSense 11.5(1) supports recording of media streams over IPv6. For Unified Communications Manager built-in-bridge calls, the recordings are done over IPv6 addresses in addition to IPV4 addresses. This is a significant change as Cisco MediaSense can now record calls from endpoints that support only IPv6 addresses. Earlier, MediaSense supported recordings over IPv4-only-stack and dual-stack endpoints. The feature is an add-on support where an administrator can assign an IPv6 address to the MediaSense server, in addition to IPv4 address. The recordings thus made, can be played back or downloaded over IPv4 interfaces.

Note SIP signaling still traverses through IPv4 addresses, thus local IPv4 address is required at MediaSense end.

During a call recording, if an IPv6 address is configured at MediaSense and both IPv4 and IPv6 addresses are supported by endpoint, preference is given to the IPv6 addresses for media streams.

Secured Communication

Cisco MediaSense 11.5(1) supports secured recording through secured SIP and SRTP (Secure Real-time Transport Protocol). At the MediaSense end, secured SIP ensures that the signaling used to set up recording sessions is encrypted. Secured SIP signaling is achieved over TLS transport layer for SIP messages. Next, MediaSense negotiates SRTP streams over signaling channels, and receives and decrypts the encrypted RTP messages. The received media streams are stored in the MediaSense server in a decrypted form and are accessible through all available channels.

With the secured communication feature, MediaSense Release 11.5(1) can now support both RTP and SRTP recordings, at the same time.

Note MediaSense supports SRTP for BiB audio call recordings only.

Finesse Role-Based Access

Cisco MediaSense 11.5(1) supports role-based access for Finesse supervisors and agents. With role-based access, Finesse supervisors can monitor the recordings of only their respective teams and Finesse agents can view only their own recordings. To use role-based access, the Finesse AgentInfo gadget should always be active on the desktop of agents and supervisors. The role-based access is applicable for Finesse-integrated Contact Center only.

MediaSense supports role-based access for active recordings, associated recordings, and archived recordings. Supervisors can search for only the MediaSense-associated recordings of agents who belong to the teams for which they are primary or secondary supervisor.

Audio Streaming: Creation and Audio RTSP Playback of Playlists

Cisco MediaSense 11.5(1) provides a functionality to create a playlist to be played back in an audio format 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.

Note For MediaSense 11.5(1), the uploaded media files that are part of the audio playlists, need to have a video component.

Delete Functionality

Cisco MediaSense 11.5(1) supports the Delete functionality feature that allows you to delete a recording in Mediasense Search and Play. You can delete an erroneous recording or a recording that is no longer required. However, you can delete one recording at a time from standalone MediaSense Search and Play. To activate the Delete icon in MediaSense Search and Play, check the **Enable Delete Functionality** check box on **MediaSense Search and Play Configuration** window (**MediaSense Administration** > **MediaSense Search and Play Configuration**).

Note In case the **Enable Delete Functionality** check box is unchecked, the **Delete** icon is disabled in MediaSense Search and Play.

Single Sign On for Agents and Supervisors

Cisco MediaSense 11.5(1) supports deployments 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.

Chrome Support

Cisco MediaSense 11.5(1) supports Google Chrome browser. For more information, see the Compatibility Matrix for Cisco MediaSense.

SHA-256 Support

Cisco MediaSense 11.5(1) supports self-signed certificates with SHA-256 encryption.

ESXi 6.0 Support

Cisco MediaSense 11.5(1) supports ESXi 6.0. For more information, see the Compatibility Matrix for Cisco MediaSense.

Updated Features

None

Deprecated Features

None

Requirements for Cisco MediaSense Release 11.5(1)

These requirements and support constraints are new or have changed for MediaSense Release 11.5(1).

Platform Requirements for Cisco MediaSense Release 11.5(1)

For platform requirements, refer to http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_MediaSense.

Upgrade Requirements for Cisco MediaSense 11.5(1)

The upgrade application posted on Cisco.com can be used to directly upgrade MediaSense 10.x to 11.5(1); it cannot be used to install a new MediaSense 11.5(1) server.

Note Some Virtual Machine parameter settings have changed. Make sure that you complete the required changes as described in the Virtual Machine Parameters Settings for Refresh Upgrade section in the *Cisco MediaSense User Guide* before you perform a refresh upgrade.

You can download the file, *UCSInstall_MCP_11.5.1.10000-56.sgn.iso*, for an upgrade from the following location.

https://software.cisco.com/download/type.html?mdfid=283613140&i=rm

Note On an upgrade to release 11.5(1), the following message appears:

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

You can ignore the message as it does not impact MediaSense functionality and performance.

Supported Upgrade Paths

The following table lists the supported paths to upgrade to Cisco MediaSense 11.5(1).

Current Version	Upgrade Path	Description
Release 9.1(1)	1. First upgrade from Release 9.1(1) to Release 10.x. 2. Then upgrade directly from Release 10.x to Release 11.5(1).	A Cisco Options Package (COP) file is required to perform an upgrade from Release 9.1(1) to Release 10.x. A COP file provides a generic method to deploy Cisco software outside the normal upgrade process.
Release 10.x	Upgrade directly to Release 11.5(1).	This is a refresh upgrade as the RHEL version of the MediaSense operating system changes in Release 11.5(1).

For more information about MediaSense Upgrade, see the *Upgrade Mediasense* section of MediSense User Guide.

Important Notes

For 2 vCPU VM configuration, required RAM has been increased from 6GB to 8GB.

Removed and Unsupported Features

None

Third-Party Software Impacts

For information on third-party software, see the Compatibility Matrix for Cisco MediaSense.