ADMINISTRATOR GUIDE

EVO 4.2.3 | September 2023

HARMAN Media Suite

Customer Support

You can obtain technical support by contacting Customer Support by telephone or e-mail. We are available 24/7/365.
Please send an e-mail to: HCS-CustomerSupport@harman.com OR
Call us at +1 214 396 0493 or US Toll Free Number +1 855 394 1543

Before contacting Harman International support

Please gather the following information and have it ready. This will help us service your request immediately:

- **a** HARMAN channel version for each module being used
- **b** Sequence of events leading to the issue
- **c** Error messages received along with the time and date that you received them
- **d** Environment details (number of transmitters, type of transmitters, number of endpoints, Operating System from servers and endpoints, Database version)
- **e** Details about the problem
- **f** Screenshots of errors
- **g** Attachments of relevant logs and configuration files

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to HCS-CustomerSupport@harman.com.

HARMAN Support

Visit the HARMAN Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

Before You Begin

Topics:

- HARMAN Support

This section describes the various editions of the HARMAN Media Suite, the audience, purpose, required skills, and related documentation.

HARMAN Support

The HARMAN Media Suite is now available as a part of HARMAN. If the HARMAN Media Suite has been upgraded from a prior software version, the system uses an Activation Key obtained from HARMAN Support by emailing HCS-CustomerSupport@harman.com.

Getting Started with the HARMAN Media Suite

Topics:

The HARMAN Media Suite product is a video content management solution that integrates with standards-based and telepresence video conferencing systems.

Important Safeguards for the HARMAN Media Suite

Read and understand the following instructions before using the system:•

- DOs
  - Close supervision is necessary when the system is used by or near children. Do not leave unattended while in use.
  - Only use electrical extension cords with a current rating at least equal to that of the system.
  - Always disconnect the system from power before cleaning and servicing and when not in use.
  - Connect this appliance to a grounded outlet.
  - Only connect the system to surge protected power outlets.
  - Keep ventilation openings free of any obstructions.
  - If the system or any accessories are installed in an enclosed space such as a cabinet, ensure that the air temperature in the enclosure does not exceed 40°C (104° F). You may need to provide forced cooling to keep the equipment within its operating temperature range.
  - Only use this product below the altitude of 2000 meters (6,562 feet).
  - Only for the non-tropical climate conditions for safe use.
  - No user serviceable parts are contained within the device.
- Don'ts
  - Do not spray liquids directly onto the system when cleaning. Always apply the liquid first to a static-free cloth.
  - Do not immerse the system in any liquid or place any liquids on it.
  - Do not disassemble this system. To reduce the risk of shock and to maintain the warranty on the system, a qualified technician must perform service or repair work.
  - Do not use this product near water.
  - Do not use this product during an electrical storm. There may be a remote risk of electric shock from lighting.

- According to the official documentation of VMware, the Snapshot function impacts the performance of a virtual machine. It is advised not to take a snapshot during normal operation of the HARMAN Media Suite (such operations are Calls/Streaming/Transcoding/Backup).

Note: Replace lithium cell carefully

The device contains a lithium cell. There is a risk of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to manufacturer's instructions.

About the HARMAN Media Suite System

As a native part of the Clariti solution, the HARMAN Media Suite product can record or live stream meetings, manage archives, and play back recordings on a variety of client devices including tablets, smartphones, desktop and laptop computers, and standards-based video endpoints.

By leveraging the HARMAN Media Suite with existing telepresence systems, video conferencing endpoints and video infrastructure, or familiar unified communications (UC) tools, your organization can easily convert real-time conferences and events into reusable multimedia assets.

HARMAN Media Suite Features

The HARMAN Media Suite has the following features:

- Integrates with endpoints, conference platforms, and other standards-based video endpoints for automated recording and playback.
- Provides Video Content Management functions with built-in tools.
- Supports SIP and H.323 standards for interoperability with third-party conferencing systems.
- Accommodates different recording and streaming ports with licenses. Optional licenses can be added for Pro and Platinum features.
- Outputs a maximum stream (live or video on demand) of 1080p HD (people+content combined).
- Provides content editing and management functions.
- Provides access to live and video call archive streams on devices with compatible browsers including PC, MAC, iOS, and Android devices.
- Enables access to video call archives through any standard-based endpoint.
- Provides REST API support for third-party integrations.
- Supports LMS/LTI integration (LTI v1.3, Deep Linking v2)
- Accepts Media Streams over RTSP/RTMP from video encoders and IP Cameras; records and live stream such inputs.
- Supports IPv6 network (except SMTP, SNMP which will be supported in a future release)

HARMAN Media Suite Capacity

The license that you buy determines the HARMAN Media Suite capacity.

This section describes the following modes of capacity available for the HARMAN Media Suite.

HARMAN Media Suite Capacity in Standalone Mode

HARMAN Media Suite Virtual Edition Capacity

Feature	Description	Maximum Record Port			
		6/3 model	12/6 model	18/9 model	40/0 model
Signaling Connection (H323/SIP)	Specifies the maximum number of devices that can be connected to HARMAN Media Suite simultaneously.	6	12	18	40
Conference Recording	Specifies the maximum number of devices that HARMAN Media Suite records simultaneously.	6	12	18	40
Unicast Live Streaming and VoD	Specifies the maximum number of endpoints that can be connected to the HARMAN Media Suite to view playback simultaneously. Playback consumes live streaming port.	3	6	9	0
Unicast Live Streaming and VoD	Specifies the maximum number of web connections support by the HARMAN Media Suite to simultaneous view live streaming and/or VOD streaming.	Up to 1,000	Up to 1,000	Up to 1,000	1,000 VoD streaming sessions

The HARMAN Media Suite 40/0 is not licensed to include live unicast or live multicast streaming. For the 40/0 model, P2P and Quick Code playback features are not available because no live streaming ports are provided, therefore, there is no live streaming with the product.

HARMAN Media Suite Capacity in Scalability Mode

In scalability mode, the real capacity is controlled by the purchased license capacity and system capacity.

The system capacity is the aggregate capacity value of each standalone machine.

Maximum license capacity of the HARMAN Media Suite **in Scalability mode**

Capacity	Value
Concurrent recordings	216*

Maximum license capacity of the HARMAN Media Suite **in Scalability mode**

Capacity	Value
Concurrent live call streaming	108*
Concurrent streaming sessions	50,000

* Six nodes with 32 GB RAM / 24 Virtual Cores each could support the 216/108 license model.

Recording and live streaming from the Easy Capture application is not controlled by license capacity.

The actual system capability and license-controlled capacity may be different.

The Relationship between Media Nodes and Capacity

Concurrent Users	Minimum Recording Ports / Streaming Ports					
	6/3 model 12/6 model 18/9 model 40/0 model	**24/12 model 30/15 model 36/18 model**	**42/21 model 48/24 model 54/27 model**	**60/30 model 66/33 model 72/36 model**	**78/39 model 84/42 model 90/45 model**	**96/48 model 100/50 model**
500-1,000	1 node	2 nodes	3 nodes	4 nodes	5 nodes	6 nodes
1,001-2,000	2 nodes	2 nodes	3 nodes	4 nodes	5 nodes	6 nodes
2,001-3,000	3 nodes	3 nodes	3nodes	4 nodes	5 nodes	6 nodes
3,001-4,000	4 nodes	4 nodes	4 nodes	4 nodes	5 nodes	6 nodes
4,001-5,000	5 nodes	5 nodes	5 nodes	5 nodes	5 nodes	6 nodes
5,001-6,000	6 nodes	6 nodes	6 nodes	6 nodes	6 nodes	6 nodes
6,001-7,000	7 nodes	7 nodes	7 nodes	7 nodes	7 nodes	7 nodes
7,001-8,000	8 nodes	8 nodes	8 nodes	8 nodes	8 nodes	8 nodes
8,001-9,000	9 nodes	9 nodes	9 nodes	9 nodes	9 nodes	9 nodes
9,001-10,000	10 nodes	10 nodes	10 nodes	10 nodes	10 nodes	10 nodes
50,000	50 nodes	50 nodes	50 nodes	50 nodes	50 nodes	50 nodes

Resource Consumption

There are two types of resource used for call and live streaming: one is recording port, the other is live encoder.

For one call, no matter if it is a normal call or a P2P call, it consumes one recording port.

Live encoders are allocated for following three scenarios:

- If there is a live streaming accompanied with the call, each output bitrate consumes one live encoder. Audio only live streaming call does not occupy live streaming encoder, and consumes one recording port.
- Playback a file to meeting.

- A P2P call recording.

In addition, if a dual-window layout is enabled for live streaming, then the output video has two streams, one for people video, the other for content video. The resource must be calculated separately.

The streaming from the HARMAN Media Suite to third-party media server does not consume streaming license resource.
Dual window for content is not supported for live streaming to external media servers. Choose single window as streaming layout in recording templates which are used for live streaming to external media servers.

The number of live encoders are calculated by the bitrate and resolution of the output video. Sometimes, the live encoders should be sum-up if a call involves more than one scenario above. For example, a P2P call enables live streaming.

The mapping between bitrate and live streaming port are shown as the table below:

Bitrate/Resolution to Port Mapping

Profile	Bitrate	Resolution/ Framerate	Live Encoder for Live Streaming	Live Encoder for P2P with Live Streaming	Live Encoder for P2P without Live Streaming
MP4 high profile	128~511	4CIF/p30	1 (actual value is 0.5)	1	0.5
	512~1023	720/p30	1	2	1
	1,024~4,096	1080/p30	2	3	1
	1,728~4,096	1080/p60			
MP4 base profile or WMV	128~255	CIF/p30	1 (actual value is 0.5)	1	0.5
	256~767	4CIF/p30	1 (actual value is 0.5)	1	0.5
	768~1,727	720/p30	1	2	1
	1,728~4,096	1080/p30	2	3	1
	1,728~4,096	1080/p60			

When recording a conference, or playing back a media file, the Collaboration Server (RMX) ports are consumed according to the resolution of each video.

Example 1, in a P2P recording without live streaming, the final call negotiation rate is 512kbps, according to **Live Encoder for P2P without Live Streaming column** in the table, the live streaming port consumption is 1.

Example 2, in a P2P recording with two bitrates live streaming, the final call negotiation rate is 512kbps, and live streaming negotiation rate is 1,024kbps and 512kbps. The resource consumption is as follows:

For P2P call consumption: the recording port consumption is 1 port.

For live streaming consumption: live streaming ports consumption is based on negotiation rate. In this example, according to **Live Encoder for P2P with Live Streaming column**, 1,024kbps P2P live streaming port consumption is 3, and according to Live Encoder for **Live Streaming colum**n, 512kbps live streaming port consumption is 1. The total live streaming port consumption is 4.

The actual port consumption is also based on license capacity.

For 2/1 mode, the highest resolution for live streaming is 720p for single window, and 4CIF for dual window.

Behaviors with Inadequate Live Streaming Resources

If there are not enough streaming ports available in system for one service request, the request will be rejected.

In recording and live streaming mode, if there is not enough resource for the call and the Allow recording when live streaming could not be created is true in Call Setting from Admin Portal > Configuration, the call may be downgraded to a recording only.

If recording template enables audio only live streaming, or if audio only is disabled, but the bandwidth negotiated is below 128 KB, the call is set up to be audio only, and the audio-only live streaming works.

If the real call rate is lower than the call rate configured in the recording template, the HARMAN Media Suite system will update the streaming ports that are actually occupied. If the system finds that multiple live streams are at the same rate, it will turn off duplicate live rates to save live streaming resources, and occupied streaming ports will be updated together. If an external live media server is configured in the VRR template, the system will not turn off the duplicate live rates.

Offline Transcoding Resource Consumption

Resource management can pause and resume the offline transcoding tasks intelligently according to the hardware capacity and live streaming port usage.

Local Media Storage Consumption

Each 60-minute 512 kbps call to the HARMAN Media Suite requires about 450 MB storage (the 512 kbps call raw + the default mp4 VoD).

For 1024 kbps, the storage space is approximately double, which is 900 MB. You cannot calculate an accurate ratio because the size also depends on the call speed, video quality, and amount of motion.

The storage capacity can be expanded on appliances using NFS storage.

Storage Usage

Situation	Primary Rate	Call Duration	Storage Space (WMV)	Storage Space (MP4)
1*1080p	1024 kbps (MP4) 1728 kbps (WMV)	60 minutes	~1.4 GB	~870 MB
1*1080p	4096 kbps	60 minutes	~3.2 GB	~3.5 GB
1*720p	4096 kbps	60 minutes	~3.2 GB	~3.5 GB
1*720p	1024 kbps	60 minutes	~862 MB	~860 MB
1*4CIF	512 kbps	60 minutes	~458 MB	~459 MB
1*CIF	128 kbps	60 minutes	~100 MB	~103 MB

People and Content Video Codecs

Situation	People Video	Content Video
Call Protocols	H.323, SIP	H.239, BFCP
Audio Protocols/Codecs	G.711, G.722, G.722.1, G.722.1.C, G.729A, Siren 14 (Mono, Stereo), Siren 22 (Mono, Stereo), Siren LPR, Siren LPRStereo	N/A
Video Codecs	H.264 BP, H.264 HP, H.263, H.263+, H.261, RTV	H.264 BP, H.264 HP, H.263, H.263+, RTV
Video Resolutions	1080P60, 1080P30, 720P, 4CIF, CIF	H.263: XGA (30) H.264: 1080P60, 1080P30, 720P30

Approximate Capacity of HARMAN Media Suite in Hours of Recording

Resolution	Call speed (Kbps)	Approx. file size of 1 hour @MP4, in MB (from Admin Guide)	Approx. number of hours of recording/TB of storage	Approx. capacity of HARMAN Media Suite Appliance Local storage, in hours (Capacity=3.5 TB)
CIF	128	103	9,700	33,950
4CIF/SD	512	459	2,170	7,595
720p30	1,024	860	1,160	4,060
1080p30	1,024	870	1,140	3,990
720p30	4,096	3,500	280	980
1080p30	4,096	3,500	280	980

HARMAN Media Suite Standalone Unicast Live Streaming and VoD

The HARMAN Media Suite is licensed for 500 simultaneous viewings of live and VoD streams from the user portal.

The HARMAN Media Suite system supports a maximum number of simultaneous live or VoD streams of up to 1,000 from the user portal with the purchase of a stream upgrade option.

Note:
As the different browsers have different session handling mechanism, which causes streaming session count calculation inaccurate. It is not recommended to watch videos through multiple tabs in one browser, it is advised to watch a video only in one tab in one browser application instance.

Stream Rate on User Portal (kbps)	Number of Simultaneous Streams from HARMAN Media Suite User Portal	License	Upgradeable to Maximum Simultaneous Streams
128~512	500 streams	Included with base system	1,000 streams
513~1,024	250 streams	Included with base system	500 streams
1,025~1,536	166 streams	Included with base system	334 streams

Stream Rate on User Portal (kbps)	Number of Simultaneous Streams from HARMAN Media Suite User Portal	License	Upgradeable to Maximum Simultaneous Streams
1,537~2,048	125 streams	Included with base system	250 streams
2,049~2,560	100 streams	Included with base system	200 streams
2,561~3,072	83 streams	Included with base system	166 streams
3,073~3,584	71 streams	Included with base system	142 streams
3,585~4,096	62 streams	Included with base system	125 streams

Multiuser Login Capacity

The maximum number of Admin Portal sessions is 200.

The maximum number of User Portal sessions is 10,000. If the license supports 50,000 concurrent streaming sessions, at least five devices including HARMAN Media Suite Center and Media Nodes should enable the Portal Server.

Navigating in the HARMAN Media Suite System

The HARMAN Media Suite provides four user interfaces that are used for specific purposes:

- Web-based admin portal
- Web-based user portal
- TV user interface
- Console

This Administrator Guide covers only the Web-based admin portal and Console user interfaces. For information on how to use the Web-based user portal and TV User Interface, refer to the HARMAN Media Suite User Guide.

Accessing Web-based Admin Portal

You can access the admin portal through a compatible web browser and do the following:

- Configure the system.
- Set up recording parameters.
- Monitor system use and health.
- Dial out to endpoints to record meetings, disconnect calls in progress, and create different transcoded versions of archived calls.
- Download media files and give admin users a quick way to access and play archives and live streams.
- Manage archives, including download media files, dynamic transcoding, play, and delete.

The HARMAN Media Suite system allows up to 200 users with admin rights to log in to the admin portal at the same time.

Note:

- It is strongly recommended for admin users to access the Admin Portal over HTTPS only.
- If the admin user accesses the Admin Portal over HTTP, it is advised to close the browser after logging out or after being logged-out due to session-timeout.
- If the admin user accesses the Admin Portal over HTTP, and the MediaSuite server is restarted (due to activate/upgrade/reboot), it is required to close the browser and re-login.
- If the admin user wants to switch between HTTPS to HTTP or vice-versa, the admin user must first logout and close the browser used over one protocol, and then reopen the browser for accessing the Admin Portal over other protocol.

Admin Portal Languages

The HARMAN Media Suite Admin Portal is available in the following languages, and you can change the Admin Portal language before you log in or after you log in.

- English
- Simplified Chinese
- Traditional Chinese
- French
- Deutsch
- Japanese
- Korean
- Spanish
- Russian
- Portuguese

Procedure:

Before you log in:

At the top-right of the login page, click the Language drop-down list and select a language.

After you log in:

1. At the top-right of the main page, click the **login administrator** drop-down list.
2. Select the option **Change Language**.
3. Click the **Preferred Language** drop-down list from the pop-up frame and select a language.
4. Click **OK** to save the setting, the page will be refreshed automatically and the selected language will be applied.

Note:

The language setting is based on the browser level. It will be reset to default system language once the cookie/cache of the browser has been cleared and the browser is re-launched.

Console Access

You can view and change IP settings and reboot the system from a console.

For example, you can set the DNS server, view disk space usage, and shut down the system.

For the HARMAN Media Suite, Appliance Edition, you can access the console through the system VGA interface on SSH. For the HARMAN Media Suite, Virtual Edition, you can access through the vSphere client console or SSH.

The user name and initial password to access console are harman/harman. You must change the initial password when you log into the console first time.

License Management

Topics:

- HARMAN Media Suite License Capacity

You must have a license to use the HARMAN Media Suite.

HARMAN Media Suite License Capacity

The license type determines HARMAN Media Suite capability.

HARMAN Media Suite License Capacity for HARMAN Activation Key Mode

License Type	Supported Calls	Supported streamings	Supported Formats
2/1	2 SIP or H.323 calls	1x720p live streaming	MP4 and WMV formats
6/3	6 SIP or H.323 calls	3x720p live streaming	
12/6	12 SIP or H.323 calls	6x720p live streaming	
18/9	18 SIP or H.323 calls	9x720p live streaming	
40/0	40 SIP or H.323 calls	None	

Activate HARMAN Media Suite Licenses through Activation Key

To activate the HARMAN Media Suite using Activation Key, you must get a product activation key from HARMAN to activate all the features. A new installation of HARMAN Media Suite Virtual Edition comes with a 30-day trial license which provides 6/3 capacity and Platinum license functionality (except the Scalability feature).

Procedure

1. Obtain the serial number and write it down for later use:
   - HARMAN Media Suite, Appliance Edition: Obtain the serial number from rear panel of the HARMAN Media Suite system.
   - HARMAN Media Suite, Virtual Edition: On the HARMAN Media Suite Admin Portal, go to **Admin > Product Activation** to obtain the serial number.
2. Provide the serial number to the Harman support at HCS-CustomerSupport@harman.com and ask for activation key.
3. The HARMAN Media suite support will revert with the activation key.

4 On the HARMAN Media Suite Admin Portal, go to **Admin> Product Activation** and select **Activation Key**.

5 Enter the activation key and click on the **Activate** button to activate the license.

Note: When a VE instance license is a trial license, consider the following points:

- Cannot restore media file into the system but can back up the media file.
- Cannot import media file into the system but can export the media file from the system.
- Cannot import configure data into the system but can export date configured from the system.
- The media storage (NFS, local storage, or AWS EBS) on instance1 cannot be synced into another trial instance, and it will be synced into instance1.

View HARMAN Media Suite License Status

You can view the status of HARMAN Media Suite licenses at any time. A feature's active status is indicated with the green icon and the inactive status is indicated with the red icon

Procedure

1 Go to **Admin > Product Activation**.

The following system information displays:

Parameter	Description
License Status	Shows the license type: Trial, Invalid, permanent, or Activated.
Software Version	Current version of the software running on the system
Serial Number	Product serial number
Activation Status	Indicates if the system is activated. After the system is successfully activated, **Active** displays.
Max Recording Ports	Maximum number of recording ports supported by the system
Max Live Streaming Ports	Maximum number of live streaming ports supported by the system
Max Streaming Sessions	Maximum number of video-on-demand and live streaming sessions supported by the system. Base: 500. **Note**: After purchasing and activating the license, the streaming sessions capacity will be increased from 500 to 1,000.
Media Encryption	Whether the AES encryption function of the system is activated.
Streaming without recording (No archive)	Whether the streaming without recording function of the system is activated. Once this function is activated, the system performs live streaming without recording and leaves no archives.
1080p 60	Whether the 1080p 60 is activated.

Parameter	Description
Timecode Watermark	Whether the basic timecode watermark capability for transcoded mp4 on-demand files is activated. On-demand archives can be output with basic timecode watermarking.
Scalability Enabled	Whether Scalability Mode is activated. This is a chargeable function and has to be purchased separately in order to use it. This feature is integrated with the license (Pro/Platinum) that you would have purchased and can be used once activated.
Platinum Enabled	Whether Platinum license is activated.
PRO Enabled	Whether PRO license is activated.
GoToMeeting	Whether GoToMeeting license is activated. This is a chargeable function, which you can use only after purchasing the **Pro / Platinum** license and activating it.
BlueJeans	Whether BlueJeans license is activated. This is a chargeable function, which you can use only after purchasing the **Pro / Platinum** license and activating it.
WebexMeeting	Whether WebexMeeting license is activated. This is a chargeable function, which you can use only after purchasing the **Pro / Platinum** license and activating it.
ZoomMeeting	Whether Zoom license is activated. This is a chargeable function, which you can use only after purchasing the **Pro / Platinum** license and activating it.
LTI Support	Whether Learning Tool Interoperability support is activated. This is a chargeable function, which you can use only after purchasing the **Pro / Platinum** license and activating it.
SAFR Feature	Whether SAFR Facial Recognition feature is activated. This is a chargeable function, which you can use only after purchasing the **Platinum** license and activating it.

HARMAN Media Suite Appliance Edition Hardware Installation

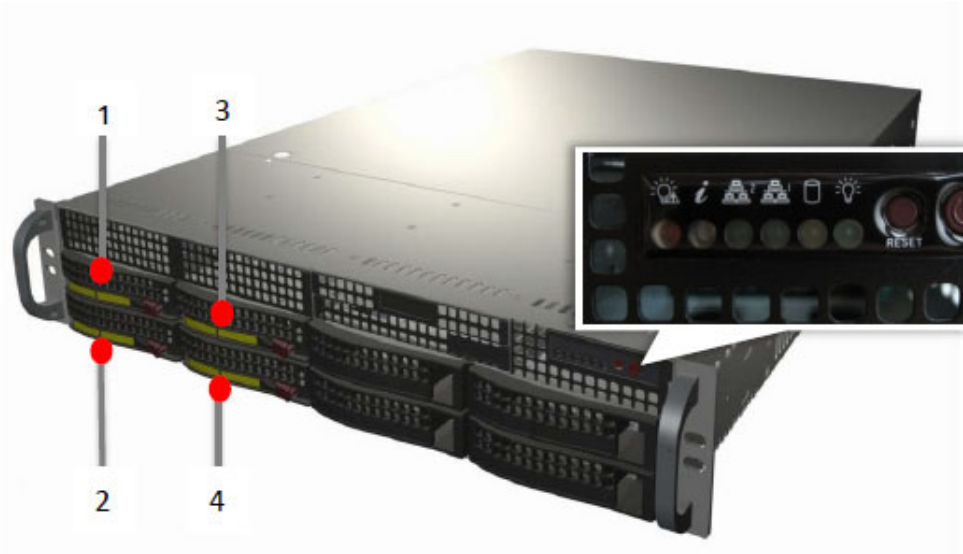
Topics:

The hardware of HARMAN Media Suite, Appliance Edition is HARMAN Capture Server. This section introduces HARMAN Capture Server appearance and hardware installation.

HARMAN Media Suite Capture Front Panel

The front panel of the HARMAN Media Suite Capture Server system is shown next.

Media Suite Capture Server **Front Panel**



There are two buttons located on the front of the chassis as described next:

Button	Name	Description
	Reset	Use the reset button to reboot the system.
	Power ON/OFF	Use the Power button to apply or turn off the main system power. Turning off the system with this button removes the main power but keeps the standby power supply.

There are six LEDs located on the front of the chassis as described next:

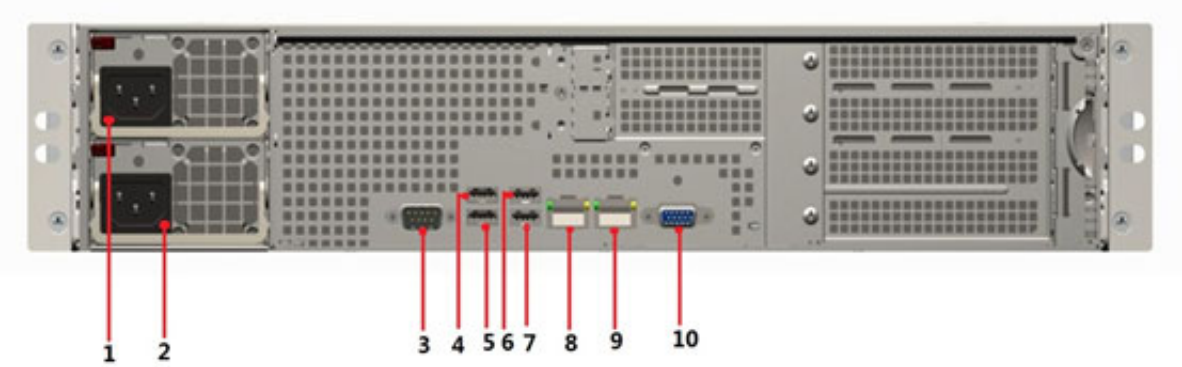
LED	Description	Panel Identifier	Status	Color
LAN1	LAN1 Activity Status Indicator		Link	Green
			Activity	Green Blink
			No Link	Off
LAN2	LAN2 Activity Status Indicator		Link	Green
			Activity	Green Blink
			No Link	Off
Status	System Status		System On (Normal)	Green
			System off	Off
HDD	Hard Drive Status		Activity	Green
Power	Power Fail		Normal	Off
			A Power Supply Module Failed	Red
Overheat/ Fan Fail	system overheat or Fan Fail		Normal	Off
			Overheat	Red
			Fan Failure	Red Blink

There are four HDDs located on the front of the chassis as described next:

No.	Port	Description
1	HDD 1	Hard Disk 1 for storage data
2	HDD 2	Hard Disk 2 for storage data
3	HDD 3	Hard Disk 3 for storage data
4	HDD 4	Hard Disk 4 for storage data

HARMAN Media Suite Capture Server Rear Panel

Media Suite Capture Server **Rear panel**



No.	Port	Description
1	Power socket and fan	Built-in power socket and fan
2 (optional)	Power socket and fan	Built-in power socket and fan Note: Available as part of the redundancy kit.
3	Serial (RS 232)	Disabled
4	USB 1	For USB device connection
5	USB 2	For USB device connection
6	USB 3	For USB device connection
7	USB 4	For USB device connection
8	LAN 1	For management network connection when network separation is enabled. The port type is 10/100/1000 Mbps. By default, LAN1 is for all management, signaling and media network connections.
9	LAN 2	For signaling network connection when network separation is enabled. The port type is 10/100/1000 Mbps. LAN2 is disabled by default.
10	VGA	Diagnostics only

Hardware Specifications

The following tables show the hardware specifications of the HARMAN Media Suite Capture Server without DSP and for the customer based in China only.

Hardware Specifications (Without DSP)

Component	Description
Chassis	Supermicro X9DRW-iF MB and Chassis
CPU	Intel® Xeon® Processor E5-2620 *2, 15M Cache,2.0GHz, 6 cores, FCLGA2011
RAM	32GB DDR3-1333 ECC Registered memory (8 x 4GB RDIMM)
System storage	Intel® SSD 520 Series (120GB, 2.5in SATA 6Gb/s, 25nm, MLC) 7mm used for system image and database.
Local media storage	3.5" Hard disk, 2T*4, SATA-3 6.0Gbps, 7200RPM, 64MB cache removable hard disk with RAID 10.
Meridian Card	N/A

Hardware Specifications (For Specific Marketing)

Component	Description
Chassis	Supermicro X9DRW-iF MB and Chassis
CPU	Intel® Xeon® Processor E5-2620, 15M Cache,2.0GHz, 6 cores, FCLGA2011
RAM	16GB DDR3-1333 ECC Registered memory (4x 4GB RDIMM)
System storage	Intel® SSD 520 Series (120GB, 2.5in SATA 6Gb/s, 25nm, MLC) 7mm used for system image and database.
Local media storage	3.5" Hard disk, 2T*2, SATA-3 6.0Gbps, 7200RPM, 64MB cache removable hard disk with RAID 1.
Meridian Card	N/A

HARMAN Media Suite Capture Server Hardware Installation

Before you begin installing this product, make sure you follow these rules to ensure general safety:

- Keep the area around the HARMAN Capture Server unit clean, free of clutter, and well ventilated.
- Choose a suitable location for the equipment rack that will hold the unit and ensure that it is near a grounded power outlet.
- Use a regulating UPS (uninterruptible power supply) to protect the HARMAN Capture Server unit from power surges and voltage spikes, and to keep it operating in case of a power failure.

Unpacking the HARMAN Media Suite

When you unpack the HARMAN Capture Server package, ensure the following items are included and in proper condition:

- One HARMAN Capture Server appliance (weighs about 50 lbs)
- Rail-mount kit for standard 19-inch equipment rack
- One power cable for your regional power
- One HARMAN Capture Server faceplate
- Two RJ-45 network cables
- Documentation DVD, which contains the links to the latest HARMAN Media Suite documentation on the HARMAN Support.
- License information

Note: In case of damaged items

If you find damage, file a claim with the delivery carrier. HARMAN is not responsible for damage sustained during shipment of this product.

Install the HARMAN Media Suite Capture Server

After you unpack and examine the components, you can install the product.

Procedure

1. Place the HARMAN Media Suite Capture Server unit on a stable flat surface.
2. Peel off the protective film from the top and bottom of the appliance.
3. If appropriate, install the rack-mount rail kit following the instructions provided.
4. Place the appliance in a properly ventilated equipment rack (shelf or rails) or similar environment.
5. Insert the power cable connector into the rear of the chassis and connect it to an appropriately rated socket outlet.
6. Connect a network cable to LAN 1 on the back of the unit.
7. Power on the system.
8. Attach the faceplate.

Note: Both power cords must be disconnected before isolating the equipment

To isolate the equipment during servicing or any time you need to physically move the appliance, if a second power supply is installed with the redundancy kit, then both power cords must be disconnected. Otherwise, the system remains energized, even with only one plug connected.

HARMAN Media Suite Software Installation

Topics:

Check the following before you install HARMAN Media Suite, Virtual Edition:

- HARMAN Media Suite Virtual Edition Software Installation
- HARMAN Media Suite License Capacity

Check the following when you install the HARMAN Media Suite, Appliance Edition:

- HARMAN Media Suite Appliance Edition Software Installation
- HARMAN Media Suite License Capacity

HARMAN Media Suite Virtual Edition Software Installation

HARMAN Media Suite, Virtual Edition is supported on VMware vSphere.

Before you install and configure the HARMAN Media Suite system, there are prerequisites to be aware of.

HARMAN Media Suite Virtual Edition Installation Prerequisites

Here are the prerequisites for HARMAN Media Suite, Virtual Edition:

- VMware vSphere client installed where you can access the ESXi host.
- Login credentials and IP addresses of one or more VMware vShpere hosts on which you will deploy your HARMAN Media Suite OVA.
- A web browser where you access the Viewer Portal. See the Web Browser and OS Requirements in the *HARMAN Media Suite Release Notes* for the supported versions.

Resource and License Management

For the first installation of HARMAN Media Suite Virtual Edition, the 30-day trial license key provides 6/3 capacity and Platinum functionality (except the Scalability feature).

To permanently enable the HARMAN Media Suite system, a HARMAN Media Suite license is required. The 2/1 model is supported for Virtual Edition only, which is different from the Appliance Edition.

Setting up VMware vSphere High Availability

HARMAN Media Suite provides High Availability (HA) by using VMware vSphere HA, which can reduce the boot time expense and shorten the failover time.

VMware vSphere HA provides availability protection between hosts in the same cluster, increases levels of availability for VMs in the same cluster, and increases business confidence in uptime for applications.

Procedure

1. Prepare three hosts:
   - Host A: create two VMs, VM1 installs vCenter, and VM2 installs DNS server (If you already have a DNS server, only need VM1).
   - Host B: installs HARMAN Media Suite Center.
   - Host C: the backup host (make sure HARMAN Media Suite Center can get the same IP at host C).
2. Setup DNS server at VM2 (If you already have a DNS server, ignore this step).
3. Install and configure vCenter in VM1.
4. Configure HA in vCenter.

For VMware vSphere HA deployment, see https://www.vmware.com/

Setting up HARMAN Media Suite in a Virtual Environment

The following steps assume you are familiar with deploying applications into a VMware environment.

For more information about deploying applications into a VMware environment, see https://www.vmware.com/

Download HARMAN Media Suite Software

Before installing the HARMAN Media Suite Virtual Edition software, you must download the software to the local storage. To download the latest software, please visit the HARMAN Media Suite Channel Store. or contact HARMAN Support by emailing HCS-CustomerSupport@harman.com

Adding a Hard Disk in VMware vShpere

HARMAN Media Suite, Virtual Edition, supports local storage as its media storage.

Make sure the OVA file has been deployed successfully.

Caution: Shut down the system before adding a hard disk in VMware vShpere

Shut down the HARMAN Media Suite system before adding a hard disk, or the system cannot run correctly.

Configure NFS

HARMAN Media Suite virtual edition supports NFS share as its media storage and local storage.

You can export an NFS share on a typical Linux distribution. HARMAN recommends to use local storage for better disk I/O performance.

Make sure that NFS is co-located on the same switch/location as the HARMAN Media Suite system, and enough CPU and memory resource to ensure stable I/O operations.

The HARMAN Media Suite system supports the following NFS:

- CentOS

- FreeNAS

Note: Windows NFS Server is not supported
Windows NFS server is not compatible with the HARMAN Media Suite.

Procedure

1 Make sure the NFS service has been installed and is running.

Examples:

```
[root@centos-nfs ~]# service nfs status
rpc.svcgssd is stopped
rpc.mountd (pid 20129) is running...
nfsd (pid 20194 20193 20192 20191 20190 20189 20188 20187) is running...
rpc.rquotad (pid 20125) is running...
```

2 Edit the NFS configuration file /etc/exports to set the file system paths for export.

Examples:

```
[root@centos-nfs ~]# cat /etc/exports
/home/nfs *(rw,no_root_squash)
/home/nfs_zip_1 192.168.9.78(rw,no_root_squash)
```

3 Restart the NFS service.

Examples:

```
[root@centos-nfs ~]# service nfs restart
Shutting down NFS daemon: [  OK  ]
Shutting down NFS mountd: [  OK  ]
Shutting down NFS quotas: [  OK  ]
Shutting down NFS services: [  OK  ]
Starting NFS services: [  OK  ]
Starting NFS quotas: [  OK  ]
Starting NFS mountd: [  OK  ]
Stopping RPC idmapd: [  OK  ]
Starting RPC idmapd: [  OK  ]
Starting NFS daemon: [  OK  ]
```

HARMAN Media Suite Docker Deployment on Azure

Topics:

Preparing Linux Environment and copy files provided by Harman

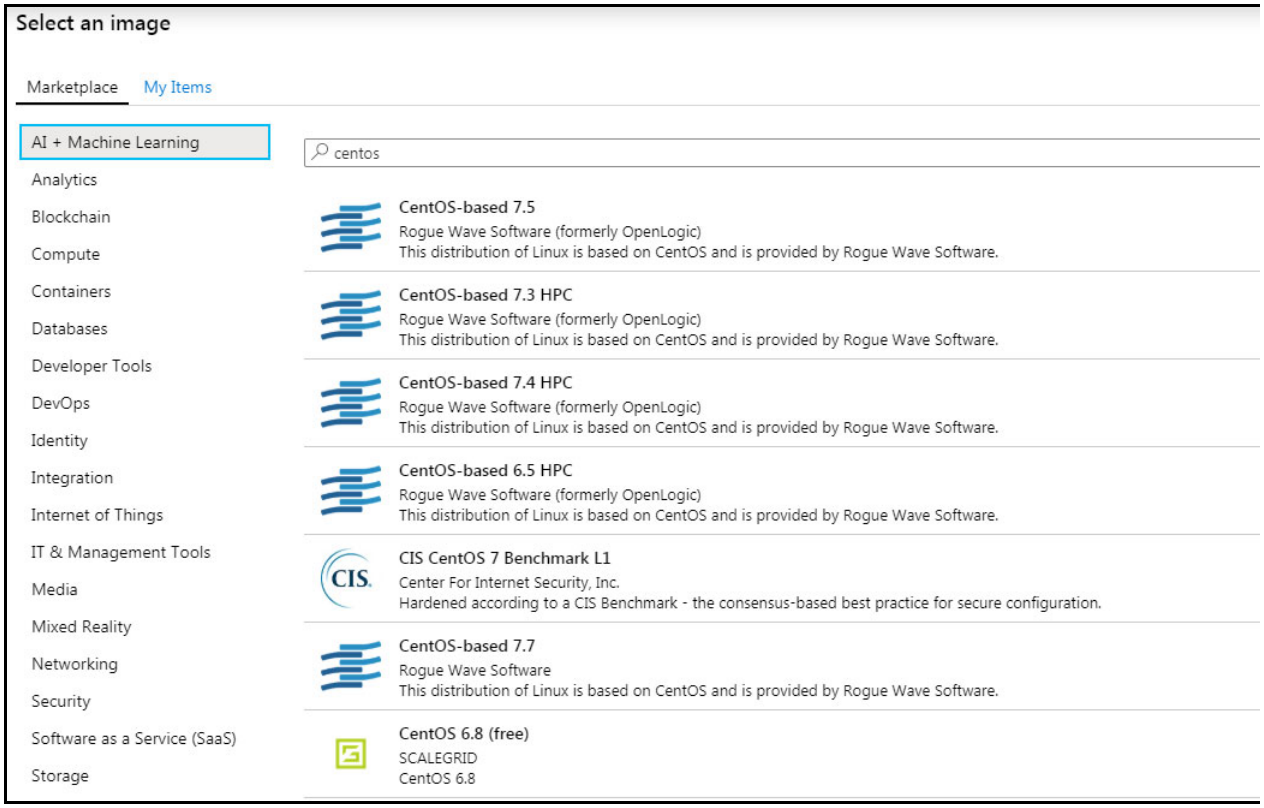
Harman provides three files to deploy the HARMAN Media Suite docker on Azure.

File name	Description
ms_docker_deploy	It is an encrypted script file, it is recommended not to modify
ms_docker_install_daemon	It needs to be placed in the same directory as the encrypted script file
azure_deploy_template	It is a template for configuration parameters. Users need to fill in their own information. Run this script to trigger deployment.
MediaSuite-3.4.0-637-2019-08-15-16-59.iso	Docker iso image file, the actual version number might vary

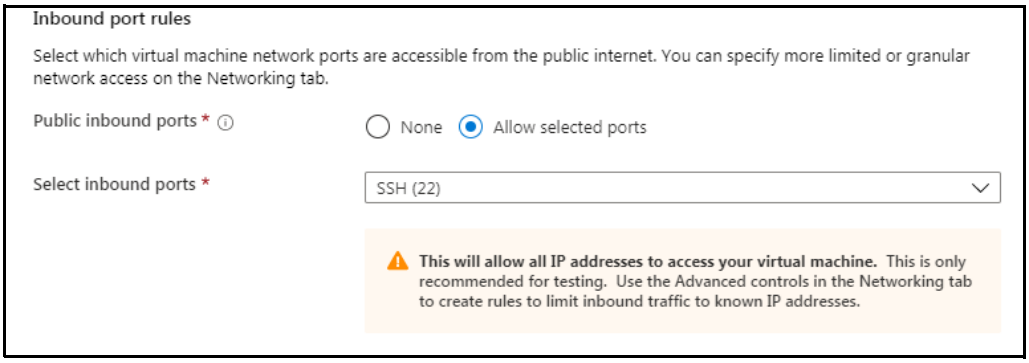
Procedure

1. As this deployment is supported only on Linux, install Linux first. You can install on local machine by Linux distribution. We recommend to use Azure to deploy a Centos on the cloud. https://docs.microsoft.com/en-us/azure/virtual-machines/linux/quick-create-portal. This is the Microsoft official guide to help you create a Linux-VM.

- Use password rather than SSH key
- Choose a Centos 7.7 image in marketplace



2 Make sure port 22 is open and created, click the review+create.



3 When you have created your Linux system, upload files to your directory. You can use the scp command or open tool winscp to upload files. When you have uploaded, login to your machine and run below commands. The following screen shows uploading done at the default path.

```
[harman@azuredeploy ~]$ pwd
/home/harman
[harman@azuredeploy ~]$ ls
azure_deploy_template  MediaSuite-3.4.0-637-2019-08-15-16-59.iso  ms_docker_deploy  ms_docker_install_daemon
```

4 Enter the password.

```
[harman@azuredeploy ~]$ sudo chmod +x ms_docker_install_daemon && sudo mv ms_docker_install_daemon /usr/bin/
[harman@azuredeploy ~]$ sudo chmod +x ms_docker_deploy && sudo mv ms_docker_deploy /usr/bin/
[harman@azuredeploy ~]$ sudo chmod +x azure_deploy_template
```

Modify Script Parameters and Run

Procedure

1 Open the **azure_deploy_template** with editor and modify the parameters.

```
#!/bin/bash

# parameters and default valume for azure deloy:
#
# ms_docker_deploy azure
#        /harman/MediaSuite-3.4.0-637-2019-08-15-16-59.iso
#        --vmname <AZ VM NAME>
#        --azgroup mediasuite
#        --azuresize Standard_A8_v2 #https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-sizes-specs
#        --azosdiskgb 100
#        --azdatadiskgb 100
#        --azusessddisk
#        --azsubnet <vnet/subnet>
#        --azlocation eastus #https://azure.microsoft.com/en-us/global-infrastructure/locations
#       --azdnsname <none>

ms_docker_deploy azure \
       /harman/MediaSuite-3.4.0-637-2019-08-15-16-59.iso \
       --vmname mymediasuite \
       --azgroup mymediasuite \
       --azuresize Standard_A8_v2 \
       --azosdiskgb 100 \
       --azdatadiskgb 100 \
       --azlocation eastus \
       --azdnsname mymediasuite
```

Parameter name	Description	Mandatory/Optional
/harman/MediaSuite-3.4.0-637-2019-08-15-16-59.iso	The image file path. In this case, it should be /home/harman/MediaSuite-3.4.0-637-2019-08-15-16-59.iso.	Mandatory
--vmname	Virtual machine name	Mandatory
--azgroup	Your Azure resource group. If it does not exist, it will be created.	Mandatory

Parameter name	Description	Mandatory/Optional
--azuresize	Virtual machine size, including CPU, memory, IO performance, etc. You can refer to the Microsoft Official link in the script to determine size.	Mandatory
--azosdiskgb	The operation system disk size. The unit is GB. The default value is 100.	Mandatory
--azdatadiskgb	The media disk size. The unit is GB. The default value is 100.	Mandatory
--azusessddisk	If you add this parameters, the disk will use SSD. Otherwise, use a standard HDD disk.	Optional
--azlocation	Where you want to deploy. You can also refer to the link for the support locations.	Mandatory
-- azdnsname	dns name	Optional

2 After filling in the parameters, run the script.

```
[harman@azuredeploy ~]$ ./azure_deploy_template
/usr/bin/az
prepare create docker machine...
Please run 'az login' to setup account.
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code G4LH8AFTM to authenticate.
```

First, the program requests Microsoft authentication. Copy the link https://microsoft.com/devicelogin in your browser and enter the code to authenticate. The authentication success page appears as shown below.

3 Wait for the deployment to finish.

```
Reboot Azure VM --image Openlogic:CentOS:7.7:latest(52.174.177.25) to start MediaSuite...
Deploy MediaSuite success on Azure VM --image Openlogic:CentOS:7.7:latest(52.174.177.25)
azure MediaSuite done, please use below IP addressin browser to login:
52.174.177.25
```

After successful deployment, you can use this address to access the HARMAN Media Suite. Wait for the HARMAN Media Suite to start.

Network Configuration

Topics:

This section describes the network settings required for the HARMAN Media Suite.

Configure Signaling Settings

For H.323, if a gatekeeper is configured on your network, you can register HARMAN Media Suite to the gatekeeper to simplify calling. A gatekeeper manages functions such as bandwidth and admission control, and also handles address translation, which allows you to make calls using static aliases instead of IP addresses that may change each day.

If you make SIP calls, you can register HARMAN Media Suite to a SIP server to simplify calling.

The template value will override the system value set under Configuration > Call Settings on the admin portal.

Configure the H.323 Call

If your network supports H.323, you can register HARMAN Media Suite to a H.323 gatekeeper to simplify calling.

Procedure

1. Go to **Configuration > Signaling Settings > H.323**.
2. Select **Register To Gatekeeper**.
3. Configure the settings listed in the following table.

H.323 Gatekeeper Settings.

Setting	Description
Gatekeeper Type	Choose between **Poly** and **Cisco VCS**.
Primary Gatekeeper	Indicates whether the system is registered to the primary gatekeeper.
Gatekeeper Address	Specify the IP address for the gatekeeper. Note: Never enter HARMAN Media Suite IP address.
Gatekeeper Port	Specify the port number for the gatekeeper (the default value is 1719).
Register User Information for Gatekeeper	Specify whether to register the system to a Poly Gatekeeper server for H.235.0 authentication. When H.235.0 authentication is enabled, the gatekeeper ensures that only trusted endpoints are allowed to access the gatekeeper.
Gatekeeper User	Specify the user name for registration with the Poly Gatekeeper server.
Gatekeeper Password	Specify the password for registration with the Poly Gatekeeper server.
Alternate Gatekeeper	Indicates whether the system is registered to the alternate gatekeeper. **Note**: The alternate gatekeeper is used only when the primary gatekeeper is not available.
System Prefix / E.164	Specify the E.164 number for the system.
System H.323 Alias	Specify the H.323 alias for the system.
Remote Display Name	Specify the name to be displayed to the far end. **Note**: If you set the remote display name with dual-bytes characters like Chinese, you will not see the characters on the far end endpoints in a H.323 call between endpoints and the HARMAN Media Suite system.

4 Click **OK**.

Configure the SIP Call

If your network supports SIP, you can use SIP to connect video calls or record Microsoft Skype for Business meetings. HARMAN Media Suite supports SIP integration with SIP servers such as the Poly DMA.

Procedure

1 Go to **Configuration > Signaling Settings > SIP**.

2 Configure the SIP settings, as shown next:

SIP Configuration Settings

Setting	Description
Transport Type	Specify the transport layer protocol used for communicating with the SIP server. It needs to be consistent with the protocol supported by the SIP server.
Enable Certificate Validation	Specify whether to validate the server's certificate before accepting it. This option is available only after you select **TLS** as the **Transport Type**. **Note**: HARMAN Media Suite always sends its own certificate to the server, regardless of this selection.
Register to SIP Server	Specify whether to register the system to the SIP server.
SIP Server Type	Choose a SIP server type from the drop-down list. If you want to record a Microsoft Skype for Business meeting, choose Microsoft Lync as SIP server. If **Microsoft Lync** is selected, the Outbound Proxy Server must be configured.
SIP Server Status	Specify: • **Server Address** • **Server Port** • **Server Domain Name** **Note**: Never enter HARMAN Media Suite IP for the **Server Address**.
Service GRUU of Lync	Enter the GRUU which can get from Skype for Business.
Register User's Information	Specify: • **User Name** • **Auth User Name** • **User Auth Password**
Outbound Proxy Server	For communication with the SIP server when the system is configured on the internal network, an outbound proxy server is required to implement traversal of the firewall or NAT. In this case, you need to set the IP address and port number for the outbound proxy server. • **Server Address:** Enter an address of the SIP server. • **Server Port**: Enter the port of the SIP server. Outbound Proxy Server must be configured for Skype for business deployment. For other SIP proxy server, Harman does not recommend to configure Outbound Proxy Server. If the HARMAN Media Suite registers to Skype for Business server with multiple front end servers in Skype for Business pool, the outbound proxy server address must be one Skype for Business front end server address, and cannot be the Skype for Business pool address.

3 Click **OK**.

Get the Service GRUU of Skype for Business

Get the service GRUU from Skype for Business for SIP setting.

Procedure

1. Run the following command from the Skype for Business server.

```
Get-CSTrustedApplication | Where-Object {$_.TrustedApplicationPoolFqdn -eq "FQDN of the HARMAN Media Suite"}
```

For example

If the FQDN of the HARMAN Media Suite is ms20713.sfb2015.com, run the following command:

```
C:\Users\administrator.SFB2015> Get-CSTrustedApplication | WhereObject {$_.TrustedApplicationPoolFqdn -eq "ms20713.sfb2015.com"} Identity : ms20713.sfb2015.com/urn:application:ms20713 ComputerGruus : {ms20713.sfb2015.com sip:ms20713.sfb2015.com@sfb2015.com;gruu;opaque=srvr:ms20713:ObManQE9k lOU122HAYh9pwAA} ServiceGruu : sip:ms20713.sfb2015.com@sfb2015.com;gruu;opaque=srvr:ms20713:ObManQE9k lOU122HAYh9pwAA Protocol : Mtls ApplicationId : urn:application:ms20713 TrustedApplicationPoolFqdn : ms20713.sfb2015.com Port : 5061 LegacyApplicationName : ms20713
```

2. Copy the value of ServiceGruu to the Service GRUU of Lync in the HARMAN Media Suite.

Set Call Preference

You can set a signaling type as your call preference.

Procedure

1. Go to **Configuration > Signaling Settings**. You can set call preference to simplify the call signaling choice from User Portal when start the recording or create the live event from User Portal.
2. Select a signaling type from **Call Preference on User Portal** down-drop list.

   The selection depends on your network, for example, if your network only supports H.323, then you can select **H.323 only**, so that user could not set SIP as signaling type by mistake from User Portal. If **SIP and H.323** is selected, one of the signaling types should be specified when start a recording or live event from User Portal. If **SIP only** is selected, the P2P recording is disabled.

Configure Port Settings

Port Settings allow specific ports in the firewall network environment to be allocated to multimedia calls.

The recording server restarts to apply your changes.

Procedure

1. Go to **Configuration > Port Settings.**
2. Select **Enable Port Configuration**.

3 Configure the port settings, as shown next:

Port Settings

Setting	Description
TCP Ports	Specify the TCP port range. You can set the starting port number (the default value is 10,000). The ending port number is calculated automatically.
UDP Ports	Specify the UDP port range. You can set the starting port number (the default value is 20,000). The ending port number is calculated automatically.
Streaming Port	Specify the streaming port range. The default value is 1,640.
Multicast Port	Specify the multicast port range. The default value is 1,641.

4 Click **OK**.

Set the System Time

You also can set the HARMAN Media Suite system time from the Admin Portal.The system restarts to apply your changes.

Procedure

1 Go to **Configuration > System Time**.

2 Configure the system time settings, as shown next:

System Time Settings

Setting	Description
Time Service	Specify how to set the system time: • **Console**: Set the time manually. • **NTP Server**: Obtain the system time from a time server. **Note:** In Scalability Mode and AWS, the console cannot be used to set system time.
Date	The current system date and time. Changing the time manually is not recommended.
Time	
Time Zone	The current time zone.
NTP Server 1 and NTP server 2	Specify the address or domain name of a network time server. NTP server 2 is used only when NTP server 1 is not available. **Note:** If you set a domain name, make sure you have already set a DNS server address that can resolve this domain name in **Device > Device Setting > Network Setting**.

3 Click **OK**.

Access HARMAN Media Suite from Internet

For security consideration, HARMAN Media Suite is usually deployed in the Intranet trust zone inside the firewall. The users and endpoints in the Intranet inside the firewall can access HARMAN Media Suite to make a call for recording and view streaming through FQDN or IP address directly.

Endpoints and users in the Internet outside the firewall can access the HARMAN Media Suite for recording or viewing streaming if configured to do so.

Enable Call Recording and Live Streaming through Firewall

If the endpoints and users are in the Intranet

- Endpoints and users in the Internet can access the HARMAN Media Suite to record and live stream the meeting through configuring the mapping policy on the firewall.
- Endpoints and users watch VoD and live streaming from Internet through a firewall, including media upload.
- An internal endpoint accesses the HARMAN Media Suite from Internet to start a recording or live streaming session.

Configure the NAT Address for Internet Access

Set NAT address for endpoints to access to the HARMAN Media Suite to record the meeting from Internet.

Procedure

1. Go to **Device** > **Device Manager**.
2. Select the device entry you want to edit, and click **Edit**.
3. Select **Network Setting** > **Network Settings**.

   In Scalability Mode, the NAT address for HARMAN Media Suite Center is required, and better to configure NAT address for each Media Node that may require Internet access, for example, recording server and live streaming server.
4. Check the **NAT Public (WAN) Address**, and input the Public IP, which is used for accessing the HARMAN Media Suite from Internet.

   The FQDN must be used, if **NAT Public (WAN) Address** is configured.

Set FQDN for Internet Access

Set FQDN for endpoints to access to the HARMAN Media Suite to record the meeting from Internet.

To enable endpoints and users in Internet outside the firewall view streaming and make a call recording on the HARMAN Media Suite, you should configure the mapping policy between the HARMAN Media Suite public IP address and internal IP address on the firewall. The ports used for configuration, refer to the HARMAN Media Suite Release Notes. In scalability mode, you should configure NAT Public Address and FQDN for the HARMAN Media Suite Center and each media node individually.

Procedure

1. Go to **Device** > **Device Manager**.
2. Select one device entry you want to edit, and click **Edit**.

3 Select **Network Setting** > **General System Network Settings**.

4 Input the FQDN of HARMAN Media Suite in **FQDN**.

The FQDN is used to create DNS address records on the DNS server. Both DNS servers deployed inside and outside the firewall should configure the HARMAN Media Suite FQDN.

Set NAT Keep alive Interval

You can set the NAT keep alive interval.

Procedure

1 Go to **Configure** > **Call Settings.**

2 Check **Enable NAT** and set the **NAT Keep Alive Interval.**

In the scenario, the HARMAN Media Suite registers to the DMA, and DMA integrates with Access Director to implement the call recording from the Internet.

Portal Settings

When using HARMAN Media Manager or an other external portal to allow users to access live and on-demand streams, it is a best practice to redirect visitors from the HARMAN Media Suite User Portal to the Media Manager (or third party portal) home page.

You can also manage a session idle timeout and the maximum number of logins for both the Admin and User Portal. Configure to show both the internal and external live streaming URL.

To configure portal settings:

1 Go to **Configuration > Portal Settings**.

2 Configure the following settings:.

Parameter		Description
Redirect Settings	Redirect users attempting to connect to the User Portal	Enter a URL for visitors to redirect from HARMAN Media Suite User Portal to the Media Manager (or third party portal) home page. **Note**: A reboot may be required for the changes to take effect.
	Test	Test whether the URL works.
	Disable view permission of User Portal for anonymous user	This is enabled by default and as a result, anonymous users on User Portal do not have viewer permission. **Note**: A reboot may be required for the changes to take effect.

Parameter		Description
Session Management	Admin Portal	• **Session Idle Timeout:** specifies the number of minutes an Admin Portal session can be idle before the server cancels the session. The default value is 30. • **Session Maximum Number Per Application:** The maximum number of Admin Portal logins. The default value is 200.
	User Portal	• **Session Idle Timeout:** specifies the number of minutes a User Portal session can be idle before the server cancels the session. The default value is 30. • **Session Maximum Number Per Application:** The maximum number of User Portal logins. The range is from 10 to 10,000, and default value is 10,000. • **Session Maximum Number per Account:** specifies the maximum allowed session for User Portal access per account. Zero means no access session limitation, but the total session number cannot exceed the value in **Session Maximum Number Per Application.**

Configure Cross-Origin Resource Sharing

Cross-Origin Resource Sharing (CORS) defines a standard way in which a browser and server can interact to determine safely whether or not to allow the cross-origin request. Specifically, the browser accesses the resource on the origin domain (http://origin-domain.example), and CORS can enable or disable the resource to be fetched cross-origin from another domain (http://domain.example), which can help to prevent the cross-site scripting security issues (refer to https://www.w3.org/TR/cors/).

HARMAN Media Suite supports the CORS mechanism to configure whether the resource within the HARMAN Media Suite side is allowed to be fetched for the cross-origin request.

To configure Cross-Origin Resource Sharing:

1. Go to **Configuration** > **Portal Setting**.
2. Configure the Cross-Origin Resource Sharing.

Cross-Origin Resource Sharing

Parameter	Description
Do not allow access to the resource	Do not allow the cross-origin request to access to resource within HARMAN Media Suite. This option is the default setting. **Note**: If **Do not allow access to the resource** is selected, the archive or live streaming from HARMAN Media Suite by embedded code in an external server cannot be accessed by the user.
Allow any origin to access the resource	Allow cross-origin request to access the resource within HARMAN Media Suite resource without limitation.
Customize origin	Allow cross-origin request to access the resource within HARMAN Media Suite for the allowed origin domain list. Click **Add** to add the allowed origin domain in **Access Control Allow Origin**.

Configure QoS

Quality of Service (QoS) is very important in the transmission of high-bandwidth audio and video data. You can use QoS to test and guarantee the following settings:

- Average packet delay
- Delay variation (jitter)
- Error rate

QoS setting is only applicable for packets when recording the call, but not for packets to player.QoS settings apply to SIP and H.323 calls only, which does not apply to streaming.

To specify QoS parameters:

1. Go to **Configuration > QoS**.
2. Configure the following settings:

QoS Parameters

Parameter	Description
Enable QoS for Signaling and Media	Enables configuration of the QoS settings. If not selected, the system uses the default QoS settings.
Type	**DiffServ** and **Precedence** are two methods for encoding the packet priority. The priority set here for audio and video packets should match the priority set in the network routers. • **Differv**: Select when the network router uses **Differv** for priority encoding. If this option is selected, enter values in the **Audio** and **Video** fields. The value range is 0-63. **Note:** If you select **DiffServ** but your router does not support this standard, IP packets queue on the same communication links with data packets. This non-prioritized queuing greatly increases the latency and jitters in their delivery and can negatively impact performance. • **Precedence:** Select this option when the network router uses **Precedence** for priority encoding, or when you are not sure which method is used by the router. **Precedence** should be matched with **None** in the **ToS** field. The value range is 0-5. If this option is selected, enter values in the **Audio** and **Video** fields. The value range is 0-5. **Note: Precedence** is the default mode as it is capable of providing priority services to all types of routers and is currently the most common mechanism.
Audio / Video	Specify the priority for audio and video IP packets. The recommended priority is 4 for audio and video to ensure that the packet delay for both is the same, that audio and video packets are synchronized, and to ensure lip and audio synchronization (lip sync).

QoS Parameters

Parameter	Description
Control	Specify the priority for controlling packets.
ToS	Select the ToS (Type of Service) that defines optimization tagging for routing the conference audio and video packets. • **Delay:** The recommended default for video conferencing: prioritized audio and video packets tagged with this definition are delivered with minimal delay. • **None:** No optimization definition is applied. This is a compatibility mode in which routing is based on **Precedence** priority settings only. Select **None** if you do not know which standard your router supports.

3 Click **OK**.

The server restarts to apply your changes.

Manage Site Topology

In Scalability Mode, Media Nodes can be deployed in different sites.

Putting recording or transcoding Media Nodes at different sites helps to localize the media processing to the closest server, and avoids media transportation across locations. Deploying streaming servers at different sites and cascading the streaming servers could support a CDN-like topology to increase the streaming capacity elastically and save the bandwidth across sites.

Add a new site

You can add a new site.

Procedure

1 Go to **Site Topology** > **Sites**.

2 Click **Add** to add a new site.

3 Enter the **Site Name** and **Description**.

HARMAN recommends that you use the state or city name where Media Node is located as the site name.

4 Select the level of the site.

If the site is the parent site, select **Level-1**. If the site is the child site, select **Level-2**, and specify the parent site in **Upper Site**. The child site can always get the stream from the parent site.

5 Go to **Subnets > Add**.

6 Enter the **Subnet Name**, **IP Address**, and **Subnet Mask Length**.

You can add multiple subnets in one site to cover all users in the site.

7 Click **OK** to add the new site.

Bulk Import Sites to the Admin Portal

You can do bulk import to import the sites to the admin portal.

Prepare the Site Name, Site Description, Subnet Name, Subnet IP Address, and Subnet Mask Length as the template input.

Procedure

1. Go to **Site Topology** > **Sites**.
2. Click **Action** > **Export Template** to get the template file for the import file. The template is stored in a local folder.
3. In the Site Template, fill in the information for all the sites.
4. Click **Action** > **Import Sites**, and select the file which contains information for all the sites.
5. Click **OK**.

   The system bulk imports sites to HARMAN Media Suite.

Related Links

Working with eCDN on page 124

Add Media Node to Site

Media Nodes can be geographically divided or functionally divided into several sites.

Each site can serve different number of users. Therefore, HARMAN suggests to deploying appropriate Media Nodes to different sites according to the number of site users.

Procedure

1. Go to **Site Topology** > **Sites**.
2. Select a site to which you want to add the Media Node, and click **Edit**.
3. Click **Add** under **Subnet** to add the subnet of the Media Node. For example, if the IP address of Media Node is 192.168.10.100, you can add a subnet 192.168.10.100/32 for the Media Node.

   For example, if the IP address of media node is 192.168.10.100, you can add a subnet 192.168.10.100/32 for the media node.

   If the subnets of the site have already covered the IP address of the media node, do not to add the subnet again.

The number of the Media Nodes in one site is based on the number of users. One Media Node can support up to 1,000 streaming sessions.

Use HTTP protocol to access the website

In addition to HTTPS, you can now access the website using HTTP protocol.

Procedure

1. Go to **Configuration > Certificate Management**.
2. Select the **Enable HTTP Protocol for Server Website** check box under **Client Certificate.**

3 Click **OK**.

Configure IP Settings through Console

By default, when a new HARMAN Media Suite is started, it obtains an IP address from the DHCP server automatically.

Follow the steps here to check the IP address assigned by the DHCP server.

To set the system IP address in the HARMAN Media Suite console:

1. Connect a VGA monitor to the VGA interface of the HARMAN Media Suite system, and connect the USB keyboard to the USB interface of the HARMAN Media Suite system.
2. Open the console of your HARMAN Media Suite.

   The default IP address displayed on the console.
3. Assign the system a static IP through the HARMAN Media Suite console. If needed, modify the HARMAN Media Suite IP address in the Admin Portal.
4. Press the **Alt+F2** keys to go to the login screen.
5. Enter the user name and password (both are ***harman*** by default).
6. Change the default password when you log into the system for the first time.
7. Set HARMAN Media Suite a static IP or DHCP for the LAN interface using **Network Settings** command, refer to Configure Network Settings for details.

   Note: Get IP address from console after the DHCP setting is finished

   After the DHCP setting configuration, go to the console and get the IP address assigned by DHCP server.
8. After you set the IP, select **Yes** to reboot and save the changes.

If you change the IP settings from the HARMAN Media Suite system console, you must confirm the changes on Admin Portal to make the settings take effective.

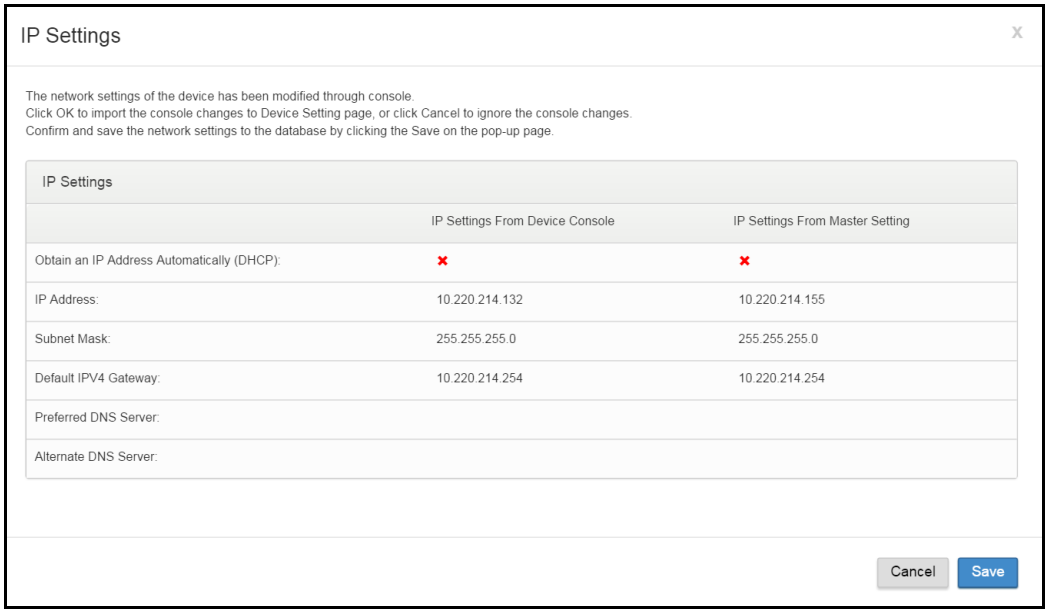
Confirm the Network Setting Changed through the Console

If the network setting is changed by console, the changes are temporary and must be confirmed through Admin Portal.

To confirm the network setting changed by console:

1. Go to **Device** > **Device Manager**.
2. Select device with ⚡ status.
3. Click **Edit** on the right corner.

4 System IP Settings window listing the network settings from displays the console and the database.



5 Click **Save** to import the network settings from the console to the Network Settings page, or click **Cancel** to keep the existing network settings.

6 Double confirm the network setting information by clicking Network Settings on the pop-up page, and click **Save** to save network settings to the database.

Customize the User Interface

Topics:

This section describes the network settings required for the HARMAN Media Suite.

You can personalize the system appearance, for example, set the IVR information and set an email address for your HARMAN Media Suite system.

Customize IVR Information

The HARMAN Media Suite system provides Interactive Voice Response (IVR) service. After the call to HARMAN Media Suite is connected, the IVR will provide information to the user about the event happening on the HARMAN Media Suite.

Procedure

1. Go to **Configuration > Customization.**
2. Select the IVR information to be played and the corresponding language option.
3. Click **Upload**.

   The audio file to be uploaded must be in PCM format, and the sampling frequency must be 16KHz, 16bit, and mono.
4. Click **Add**, select the audio file, and click **Open**.
5. Click **OK**.

Default IVR Message

Default IVR message parameters for IVR information configuration.

Default IVR Messages

Message Type	Message Text	When Played
Welcome	Welcome to conference recording playback service.	When joining the recording service where **Start Recording Immediately** is disabled.
Recording Started	Conference recording has started.	The conference recording has started.
Recording Stopped	The conference recording has ended.	The conference recording has ended.
Recording Paused	The conference recording is now paused.	The conference recording is paused.
Recording Resumed	The conference recording is now resumed.	The conference recording is resumed.
Disk Warning	You have exceeded your allocated disk space.	When there is not enough disk space to make recordings.
Call Will Be Ended Soon	The conference recording will end in another 10 minutes.	The conference recording is about to end in 10 minutes.
Playback Ended	Your playback has ended.	When the playback is ended.
Playback Not Allowed	You are not allowed to play back this archive.	You do not have permission to play back the archive after three failed attempts to input your personal code.
Playback Not Processed	Sorry, your playback request can not be processed.	When playing back an invalid archive.
Playback Paused	Your playback is paused.	When the playback is paused.
Playback Stopped	Your playback is stopped.	When the playback is stopped
Playback Session Timeout	Your session has timed out Your call will hang up.	When playing back an archive with the PIN code protection enabled, and if you do not input the PIN code within 15 seconds, or if the playback is paused for five minutes.
Input Personal Code	Please enter your personal code and then press the pound key.	When playing back an archive under PIN code protection.
Invalid Personal Code	Invalid personal code, please try again.	When play back an archive with an invalid PIN code.

Customizing UI Logo

You can customize the logo displayed on both the Admin Portal and User Portal.

To customize the logo picture of the web management interface:

1. Go to **Configuration > Customization**.
2. In the **Logo** area, click **Change Logo > Add** to select the picture to be uploaded.

   The uploaded pictures must be in the *.png format with 27 pixel height and 150 pixel to 350 pixel width.
3. Click **Open > Upload**.
4. Click **OK**.

Set up an Email Address

You can set an email address for your HARMAN Media Suite system. This is filled to “From” address in the email the system sent out.

Procedure

1. Go to **Configuration > Customization**.
2. Configure the following settings:
   - **Admin Email Settings**
     - **Sender Email:** This is filled to “From” address in the email the system sent out.
     - **Frequency:** Select the period for automatic email notification.
     - **QR Code Option**: Select the link type that is contained in QR code.
     - **Receiver Email:** Email is sent when an administrative event occurs, like disk warning, alert, etc.
     - **Enable SMTP:** Select the check box to enable SMTP.
     - **SMTP Server:** Specify the SMTP server IP address.
     - **SMTP Server Port:** Specify the SMTP server port.
     - **SMTP User Name:** Specify the SMTP user name.
     - **SMTP Password:** Specify the SMTP password.
     - **Send Test Email:** Select this check box to send a test email after applying all changes.
   - **Service Email Settings**
3. **Enable Email Notifications:** When enabled, you will receive email notifications when live streaming starts or when the archive is ready for VoD.

Securing the System

Topics:

This section deals with how to secure the HARMAN Media Suite System

Certificate Management

X.509 certificates are a security technology that assists networked computers in determining whether to trust each other. The HARMAN Media Suite system supports using X.509 certificates (version 3 or earlier) for authenticating the network connections. Once a certificate is purchased and installed in the HARMAN Media Suite system, it may be used for the following connections:

- Web server (TLS)
- Microsoft Active Directory server (LDAPS)
- SIP recording (TLS)
- FTP Server (FTPS)
- Microsoft Skype for Business

Create a Certificate Signing Request

This procedure creates a Certificate Signing Request (CSR) that you can submit to your chosen certificate authority.

Note: CSR overwrite
Creating a new CSR overwrites the existing pending CSR, if any.

To create a certificate signing request:

1. Go to **Configuration > Certificate Management**.
2. Select **Issue Signing Request**.
3. Enter the certificate information, as shown next:

Certificate Information

Parameter	Description
Common Name	Specify the name of the system. Enter the FQDN of HARMAN Media Suite.
Organizational unit (OU)	Specify the business unit defined by your organization. Use a comma (,) to separate several business units.
Organization	Specify your organization's name.
City or locality (L)	Specify the city where your organization is located (optional).
State (ST)	Specify the state or province where your organization is located (optional).
Country (C)	Specify your two-character country code.
Subject Alternative Names (SAN)	Add the SAN to Certificate. In Scalability Mode, you should add all possible FQDNs of each Media Node in this field if https is enabled. Additionally, If a new device is added, a new certificate need to be generated to include the new device.

4 Click **OK**.

The **Certificate Signing Request** dialog box displays the encoded request.

5 Copy the entire contents of the **Encoded Request** box and submit it to your CA. Be sure to include the text -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----.

Depending on the certificate authority, your CSR may be submitted by pasting it into a web page.

HARMAN Media Suite only generates SHA-2 CSR.

6 Click **OK**.

When your request has been processed, your CA sends you a signed public certificate for your HARMAN Media Suite system. Some certificate authorities also send intermediate certificates or its root certificates.

The CA might send you the certificate as email text, an email attachment, or content on a secure web page.

Install the Certificate in the System

Certificates and certificate chains are a security technology that allows networked computers to determine whether to trust each other.

By default, to support encrypted communications and establish a minimal level of trust, the system includes a default key and a signed certificate.

However, to implement a full certificate chain to a root certificate authority (CA), the system requires both a root CA certificate and an identity server certificate signed by the root CA. Therefore, at times you must request these certificates from your CA.

If HARMAN Media Suite integrates with Skype for Business or Lync, make sure to create Certificate Signing Request to trusted CA server in Skype for Business or Lync Server environment. Install certificate chain from CA server on HARMAN Media Suite.

Note: Generate a new certificate if a new Media Node is added in Scalability Mode
If a new device is added in Scalability Mode, a new certificate needs to be generated to include the new device.

Procedure

1. Install your chosen certificate authority's public certificate, if necessary, so that the HARMAN Media Suite system trusts that specific CA.
2. Create a certificate signing request to submit to the CA.
3. Install a public certificate signed by your CA that identifies the HARMAN Media Suite system.

   The HARMAN Media Suite system accepts the following types of certificate chains or single certificates:

Certificate Types

Type	Description
.pem	Privacy Enhanced Mail, base64 encoded DER certificate, enclosed between `"-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"`.
.cer, .crt, .der	Usually in binary DER form, but Base64-encoded certificates are also common (refer to .pem).
.p7b, .p7c	PKCS#7 SignedData structure with certificates or CRLs and without data.
.p12	PKCS#12, may contain public certificates and password-protected private keys.
.pfx	PFX, predecessor of PKCS#12. This type usually contains data in PKCS#12 format, for example, with PFX files generated in IIS.

Install a Certificate Authority's Certificate

You must install a CA's certificate if you don't obtain a certificate chain that includes a signed certificate for the HARMAN Media Suite system, your CA's public certificate, and any intermediate certificates.

If you are using Edge browser in Windows 10, the CA is needed or you cannot access the HARMAN Media Suite by Edge.

The certificate must be either a single X.509 certificate or a PKCS#7 certificate chain. If it is ASCII text, it's in PEM format, and starts with the text -----BEGIN CERTIFICATE-----. If it is a file, it can be either PEM or DER encoded.

Procedure

1. Go to **Configuration > Certificate Management**.
2. If you are using a certificate authority that is not listed, obtain a copy of your certificate authority's public certificate.
3. Select **Install Certificates**.
4. Do one of the following:

- Click **Upload Certificate** and click **Add** to browse to the certificate. Upload the selected certificate, and enter your password if necessary.
- Copy the certificate text, and then click **Paste Certificate** to paste it into the text box.

5 Click **OK**. If the certificate can be verified, the system installs it.

View Certificate and Certificate Details

You can review installed certificate details.

Procedure

1 Go to **Configuration > Certificate Management**.

2 Click on **Display Details**.

Certificate Details

Parameter	Description
Certificate Info	States the purpose and alias of the certificate.
Issue To	States the entity to which the certificate was issued and the certificate serial number.
Issue By	States the issuer.
Validity	States the issue and expiration dates.
Fingerprints	States SHA2 and MD5 fingerprints (checksums) for confirming certificate.

Note: Notify certificate expire day
When a certificate is about to expire, you are notified ten days prior to the expiration date.

Remove a Certificate

You can remove installed certificates.

Note: Newly installed Certificate cannot be removed
A newly installed certificate cannot be removed when it is the only private certificate that can be used as web service certificate in the system.
If you install a newly server SSL certificate, the old one will be replaced automatically.
If you want to fall back to self-signed certificate, reset configurations from console.

Procedure

1 Go to **Configuration > Certificate Management**.

2 Highlight the certificate you want to remove.

3 Click **Action > Delete**.

Use Local CRL to Obtain Revocation Status

You can enable Certificate Revocation List (CRL) to obtain the revocation status of a certificate presented to the system.

Procedure

1. Go to **Configuration > Certificate Management**.
2. Select **Enable Web Client Certificate Validation**.
3. Select **Validate by local CRL store.**
4. Click **OK**.

   The system restarts to apply your changes.

Regenerate a Default Self-Signed Certificate

You can renew self-signed certificate for the existing system.

Procedure

1. Go To **Configuration > Certificate Management**.
2. Click on **Action > Renew Self-Signed Certificate**.
3. Click **OK** to confirm the renew action.

   System must reboot to make the setting take effective

Enable Support for Self-Signed Certificates in Browsers

You need to add self-signed certificate to browser's truststore explicitly because all new browsers complain about self-signed certificates and prefer CA-signed certificates:

For Chrome

1. Open the URL **https://<SERVER_IP>** in the browser.
2. On the warning page, click on **Advanced**.
3. Click on **Proceed to <SERVER_IP> (unsafe)** to continue adding self-signed certificate into Chrome’s truststore.

For Mozilla Firefox

1. Open the URL **https://<SERVER_IP>** in the browser.
2. On the warning page, click on **Advanced**.
3. Click on **Accept the Risk and Continue** to continue adding the self-signed certificate into Firefox’s truststore.

Use OCSP to Obtain Revocation Status

You can enable Online Certificate Status Protocol (OCSP) to obtain the revocation status of a certificate presented to the system.

If the certificate includes an AIA extension, the system has the information needed to configure OCSP for obtaining revocation status.

Procedure

1. Go to **Configuration > Certificate Management**.
2. Select **Enable Web Client Certificate Validation**.
3. Select **Validate by OCSP.**
4. Click **OK**.

   The system restarts to apply your changes.

Password Settings

Go to **Configuration > Password Settings** to manage your password, change the security policies that control what kind of password you use, and how often you have to change it.

Caution: Change the account password in the integrated system if the password is changed in HARMAN Media Suite side

If HARMAN Media Suite integrates with other systems (such as Media Manager), make sure to change the password in other systems after the account password used by other systems is changed in HARMAN Media Suite. Otherwise, the account will be lockout.

Security Policy Parameters

Parameter		Description
Account Management	Failed Login Lockout Threshold	Specify the lockout times that the user inputs the wrong password continuously in a specific duration. The lockout duration can be configured in **Failed Login Lockout Duration**. Default: 3
	Failed Login Lockout Duration	Specify the lockout duration in which user inputs the wrong password specific times continuously. The lockout threshold can be configured in **Failed Login Lockout Threshold**. Administrator can unlock the users from **User** > **Users** > **Edit** >**Status**. If all Administrators are locked, system unlocks the last locked Administrator automatically after being locked out one minute later. Default: 60 minutes. If 0 is set, lockout for the failed login is disabled.

Security Policy Parameters

Parameter		Description
Password Management (takes effect on Admin Portal and User Portal)	Password Expired Warning Period	Specify how far in advance the system displays a warning that the password will expire, if the **Maximum Password Time Limit** parameter value is more than this parameter. Default: 10 days
	Maximum Password Time Limit	Specify the maximum number of days that can pass before the password must be changed. Default: 90 days
	Minimum Password Time Limit	Specify the minimum number of days that must pass before the password can be changed. Default: 0
	Reuse Number of Password	Specify the number of recent passwords that cannot be reused. For example, if set to 2, the previous two passwords cannot be reused. Default: 0

Security Policy Parameters

Parameter		Description
Password Complexity	Minimum Password Length	Specify the minimum number of characters required for a valid password. Default: 1
	Minimum Password Changed Characters	Specify the number of characters that must be different or in a different position in a new password. If this is set to 3, “123abc” can change to “345cde” but not to “234bcd”. Default: 0
	Maximum Consecutive Repeated Characters	Specify the maximum number of consecutively repeated characters in a valid password. If this is set to 3, “aaa123” is a valid password but “aaaa123” is not. Default: 0
	Minimum Upper Case	Specify the minimum number of uppercase characters required for a valid password. Default: 0
	Minimum Lower Case	Specify the minimum number of lowercase characters required for a valid password. Default: 0
	Minimum Numeric Characters	Specify the minimum number of numbers required for a valid password. Default: 0
	Minimum Special Characters	Specify the minimum number of special characters required for a valid password. Supported characters include the characters displayed in the Special Characters Set field. Default: 0

Security Policy Parameters

Parameter		Description
SSH Access	Enable the root user to access the SSH	Specify whether to allow a Linux root user to access the SSH. Only available when **Enable users to access the SSH** is enabled.
	Enable users to access the SSH	Specify whether to allow users to access the SSH. If you disable user to access the SSH, you cannot access the HARMAN Media Suite by SSH anymore, and if Admin Portal disconnects unexpectedly, the server only can be accessed through console for the Virtual Edition or VGA for the Appliance Edition. **Caution**: Change **Enable users to access the SSH** configuration will impact the network and may cause unexpected system problem. HARMAN recommends operating the command during non-busy hours for safety.
Verification Code	Enable captcha	Enable an additional verification code on the user login page. When it is enabled, the user has to input a verification code for login. Default: disabled

Note: Value 0 is no limitation
The value 0 indicates no limitation to this option.

Integrating with an Enterprise Directory

Topics:

Enterprise Directory

The HARMAN Media Suite system supports integration with a Active Directory server.

If the integrated Active Directory domain is in a forest, users from any domain in the forest can be authenticated and access User Portal directly as ordinary users. Active Directory user is also supported to access the Admin Portal, after the administrator permission is granted to the Active Directory user. The Active Directory users do not need to register in the HARMAN Media Suite system user database.

Note: Supported characters in group name
HARMAN Media Suite only supports the following symbols in the group name:
[]()$%?/@!_-

Configure an Enterprise Directory Server

You can configure an Enterprise Directory Server.

If the system is configured with an Enterprise Directory server, users defined on the Enterprise Directory can log in to the HARMAN Media Suite user portal as ordinary users.

Procedure

1. Go to **Configuration > Active Directory**.
2. Configure the following settings:

Parameter	Description
Enable Active Directory	Specify whether to enable Active Directory functionality for this system.
Active Directory Address	Set the IP address, FQDN, or domain name of the Active Directory server to be integrated. If the IWA is enabled, FQDN is required. **Note**: If you set a domain name, make sure you have already set a DNS server address in **Device > Device Setting > Network Setting** that can resolve this domain name.

Parameter	Description
Active Directory Port	Specify the port number for the Active Directory. The default value is 636.
Active Directory User	Set the user name that will be used by the HARMAN Media Suite system to access resources on the Active Directory server. The format should be *domain\user* or *user@domain.com.*
Active Directory Password	Set the user password that will be used by the HARMAN Media Suite system to access resources on the Active Directory server.
Active Directory Base DN	Can be used to restrict the HARMAN Media Suite system to work with a subset of the Active Directory (such as one tree of multiple trees, a subtree, or a domain). Leave the default setting, All Domains, initially.
Enable TLS Connection	Specify whether to enable TLS encryption for communication between the HARMAN Media Suite system and the AD server.
Synchronize AD Time Point	Specify when to synchronize AD data on a daily basis.
Test	Test whether the Active Directory server is reachable.

3 Click **OK**.

When the HARMAN Media Suite system is connected to the Active Directory server, **Active Directory Status** on the page displays **Connected**.

Configure the HARMAN Media Suite for Web Single Sign-On

HARMAN Media Suite supports Web Single Sign-On (SSO) to simplify the user login and authenticated progress.

HARMAN Media Suite can be integrated into web SSO portal as an application. The user log into web SSO portal for single authentication, and can access HARMAN Media Suite User Portal through web SSO portal without authentication.

Configure web SSO parameters

You can configure web SSO parameters.

Procedure

1 Go to **Configuration > Active Directory**.

2 Configure the following settings:

Parameter	Description
Enable SSO	Specify whether to enable SSO.
Identity of Web SSO Portal	Enter the web SSO portal identity.
Password of Web SSO Portal	Enter the web SSO portal password.

Parameter	Description
Key for AES Encryption	Enter at least 16 characters to decrypt the information send from web SSO portal.
Fieldname for User	The field name of user in the URL.
Enable timestamp validation	If enable timestamp validation, the HARMAN Media Suite involves a timestamp check, and the URL is accessible within the specified seconds. After the valid time, the HARMAN Media Suite redirects the operator to login the page.
Enforce timestamp validation within	Enter the URL valid time in second.

3 Click **OK** to finish the setting.

The HARMAN Media Suite will reboot automatically.

Configure Web SSO Portal

HARMAN Media Suite requires web SSO portal send the specific information so that users can be properly authenticated and web SSO portal can be recognized the trusted portal.

The web SSO portal should compose the URL like the following example:

```
http://<userportal
server>/userportal/SingleSignOn?HARMANuser=HARMAN\\xxx&Authorization=sso:sso&TARGET=ht
tp://mediaSuite/index.html
```

URL Items

Item	Description
HARMANuser	The string should same as the **User ID** configured in **Admin Portal** > **Configuration** > **Active Directory**.
HARMAN\\xxx	The user name who want to log into the HARMAN Media Suite User Portal. The format should be domain\user name. **Note**: “\” is the escape character, so should be changed to “\\”.
sso:sso	The string should same as **Identity of Web SSO Portal** and **Password of Web SSO Portal** in **Admin Portal** > **Configuration** > **Active Directory**.
http://mediaSuite/index.html	The URL which the user want to visit.
1494835626467	The current time in milliseconds.

The URL is encrypted by AES encryption with the CBC model, and the key is configured in **Key for AES Encryption** from **Admin Portal** > **Configuration** > **Active Directory**.

SSO via SAML (Security Assertion Markup Language)

HARMAN Media Suite supports the SSO Login via SAML 2.0 protocol for the User Portal. The SSO users will be stored in Media Suite as a local SAML user who has the basic Media Suite role as User.

Enable SSO via SAML

The SSO Login can be enabled under **Admin Portal** > **Configuration**.

Procedure

1. Click **Configuration** > **SSO via SAML**.
2. Check the option **Enable SSO via SAML**.
3. Download the **FederationMetadata.xml** of **ADFS** by visiting https://[ADFS Host IP/FQDN]/FederationMetadata/2007-06/FederationMetadata.xml
4. Open and upload the **FederationMetadata.xml**, click **OK**.
5. Wait for a few seconds and open the **SSO via SAML** configuration settings again, the **Download** button will be enabled now, click it to download the **metadata.xml** of HARMAN Media Suite.
6. Configure the **metadata.xml** of Media Suite on the ADFS server, refer to Configure ADFS for supporting SSO login via SAML

Note:

1. Currently, HARMAN Media Suite only supports IdP ADFS.
2. If we are going to change the network configuration, we need to re-configure the SSO via SAML setting.
3. **AD** and **SSO via SAM**L should be regarded as two different systems.
4. Media Suite does not directly support logout from the ADFS side.
5. SSO via SAML does not support IWA and Multiple-factor authentication.

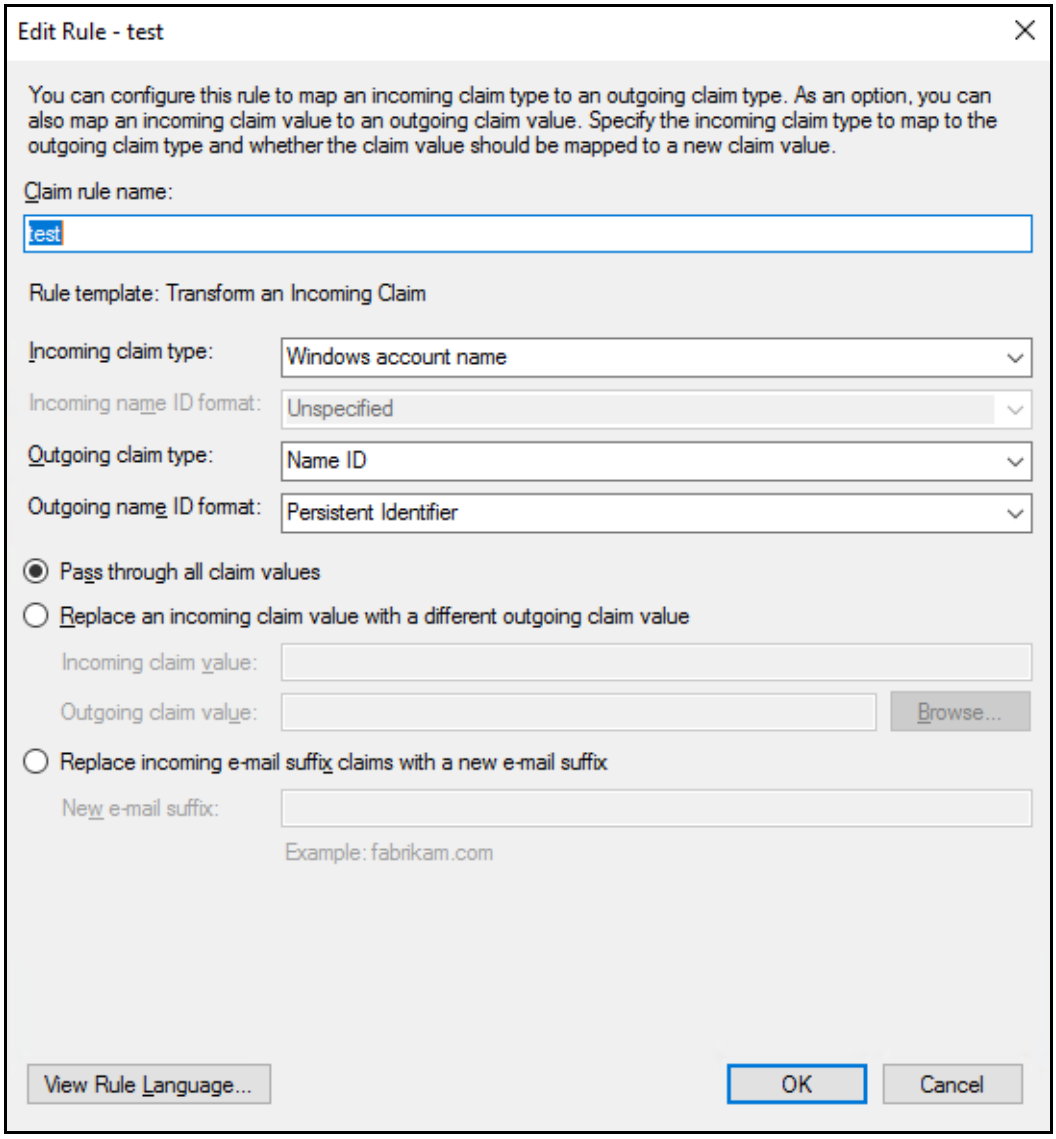
Customize SAML User Mapping

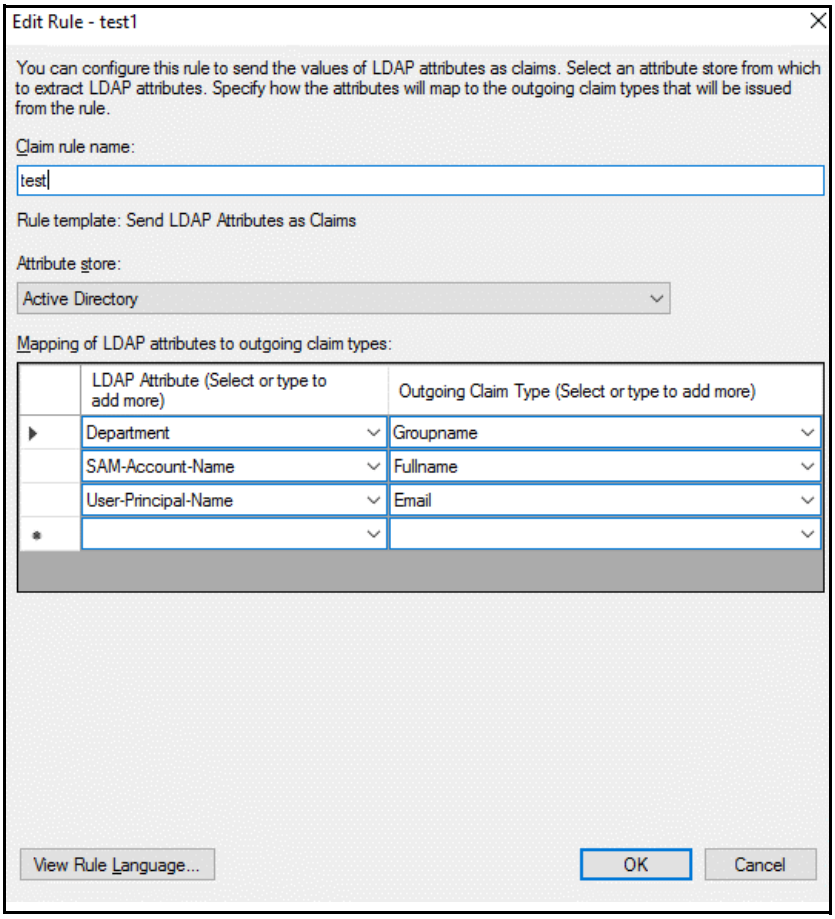
Harman Media Suite supports customizing the below fields for SAML users who will be stored in Media Suite.

Media Suite Fields	Mapped ID Fields
Username (Identifier)	Media Suite will use "Name ID" on IDP as the default username if this field is empty or the configured value is not found.
Full Name	Media Suite will use the above "Username (Identifier)" as the default Full name if this field is empty or the configured value is not found.
Email	Media Suite will not add Email if this field is empty or the configured value is not found.
Group Name	Media Suite will not add Group if this field is empty or the configured value is not found.

Example

Claim Issuance Policy on ADFS:


Edit Rule - test
You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.
Claim rule name:
test
Rule template: Transform an Incoming Claim
Incoming claim type:
Windows account name
Incoming name ID format:
Unspecified
Outgoing claim type:
Name ID
Outgoing name ID format:
Persistent Identifier
Pass through all claim values
Replace an incoming claim value with a different outgoing claim value
Incoming claim value:
Outgoing claim value:
Browse...
Replace incoming e-mail suffix claims with a new e-mail suffix
New e-mail suffix:
Example: fabrikam.com
View Rule Language...
OK
Cancel



Configuration on HARMAN Media Suite

Configure the HARMAN Media Suite for Integrated Window Authentication

HARMAN Media Suite supports Integrated Windows Authentication (IWA) to simplify the user login and authenticated progress.

If IWA is enabled, and the user logs into the proper domain on Windows clients or servers, the user can access the HARMAN Media Suite User Portal with their Windows domain and user name through browsers directly without authentication.

Before you configure IWA, you must first set up a user in your Active Directory domain for the HARMAN Media Suite. Refer to the Microsoft support site for detailed instructions and for further information regarding IWA and the requirements for using it in your Active Directory domain.

Configure Enterprise Directory for IWA

Before setting up the IWA configuration in the HARMAN Media Suite, complete the steps in your Active Directory (AD) server.

Create the Service Principal Names Associated with Enterprise Directory User Account

You can create the Service Principal Names associated with Enterprise Directory user account in Enterprise Directory Server.

Procedure

1. Log in to the AD server as Administrator.
2. Run the command in the following format to create the Service Principal Names (SPNs) associated with the AD user.

   ```
   setspn.exe -A HTTP/<Media Suite FQDN> <Active Directory user>
   ```

   The AD user must be the same as the user in the setting of **Active Directory User** in **Configure** > **Active Directory**. The FQDN must the same as the setting of **FQDN** in the **Device** > **Device Manager** > **Device Setting** > **Network Setting** > **General System Network Setting**.

   For example, if the HARMAN Media Suite FQDN is userportal.mediasuite.com and AD user is aduser, the command would be:

   setspn.exe -A HTTP/userportal.mediasuite.com aduser

   Note: Do not register HARMAN Media Suite with two different AD users

   The HARMAN Media Suite cannot be registered with two AD users. If you want to change the `AD user, run the command in the following format to remove the existing setting:`

   ```
   setspn.exe -D HTTP/<Media Suite FQDN> <Active Directory user>
   ```

Get the Active Directory Realm

Get the Enterprise Directory realm for IWA parameter configuration.

Procedure

1. Log in to the Active Directory server as Administrator.
2. Run `klist` to get the realm. The realm is case sensitive.

   The realm is used for IWA configuration on the Admin Portal.

Configure the HARMAN Media Suite for IWA

After you set up Enterprise Directory Server, you can configure the IWA on HARMAN Media Suite. If the IWA configuration is completed successfully, it attempts the IWA authentication while accessing the User Portal.

Procedure

1. Go to **Configuration > Active Directory**.
2. Configure the following settings:

Parameter	Description
Enable IWA	Specify whether to enable Integrated Windows Authentication (IWA). If IWA is enabled, the FQDN is required for **Active Directory Address** in **Active Directory**.
Active Directory Domain	Specify the active directory domain used for IWA authentication.
Active Directory Realm	Specify the active directory realm. The realm is case sensitive.

3. Click **OK** to finish the setting, and the HARMAN Media Suite will reboot automatically.

Note:
Ensure that the System time of the HARMAN Media Suite is consistent with the Active Directory Server. You must set the same NTP server for both of them.

Updating Local Intranet Zone to All Client Computers Joined to Domain

Because the User Portal is loaded as a FQDN, all the browsers place it in the Internet zone. By default, browser clients do not pass Kerberos tickets to websites in the Internet zone. You must add the User Portal FQDN to the Intranet zone in browser on each client computer joined to domain.

Working with Scalability Mode

Topics:

Scalability mode is a feature that enables multiple devices to function together.

In Scalability Mode, one HARMAN Media Suite Center and several Media Nodes work together to provide higher capacity and better management for recording, live streaming, and transcoding.

Verify Scalability Mode License

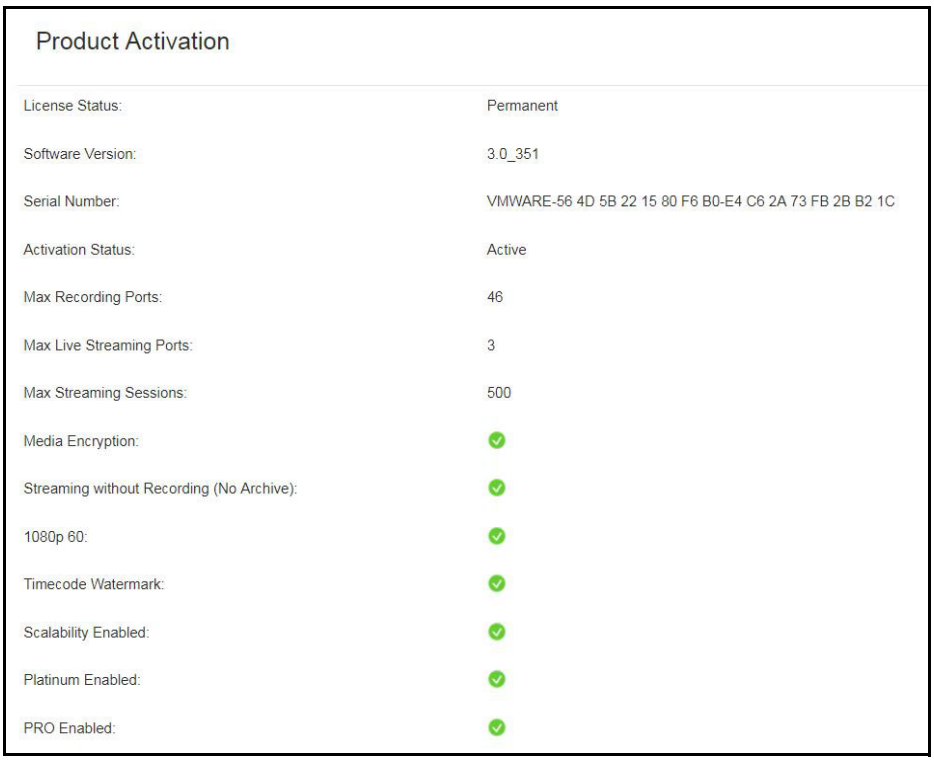
Scalability mode needs an additional scalability license to active. The scalability license has dependency on pro license which is a prerequisite to activation.

Note: Apply license to HARMAN Media Suite Center only

If HARMAN Media Suite is in Scalability Mode, license is activated on HARMAN Media Suite Center only and controlled the whole cluster.

Procedure

1. Go to **Admin** > **Product Activation**.
2. Check to ensure that **Scalability Enable** has a green check-mark next to it after the license is activated



Product Activation

License Status:	Permanent
Software Version:	3.0_351
Serial Number:	VMWARE-56 4D 5B 22 15 80 F6 B0-E4 C6 2A 73 FB 2B B2 1C
Activation Status:	Active
Max Recording Ports:	46
Max Live Streaming Ports:	3
Max Streaming Sessions:	500
Media Encryption:	✓
Streaming without Recording (No Archive):	✓
1080p 60:	✓
Timecode Watermark:	✓
Scalability Enabled:	✓
Platinum Enabled:	✓
PRO Enabled:	✓

HARMAN Media Suite Roles

In Scalability Mode, there are two types of roles in the HARMAN Media Suite: HARMAN Media Suite Center and Media nodes.

HARMAN Media Suite Center and Media Node

- HARMAN Media Suite Center role provides central control and management of the cluster, including cluster configuration, sanity monitoring, and service load balancing. In addition, HARMAN Media Suite Center provides portal access (Admin Portal and User Portal), and acts as the signaling proxy (SIP and H.323) which interfaces with external signaling networks.
- HARMAN Media Node role provides User Portal access, and media processing functionality, including recording, streaming, and transcoding. The service distribution among HARMAN Media Suite Center and Media Nodes is based on the idle capability of each device.

Set the HARMAN Media Suite Center to Media Node

You can assign a role to the HARMAN Media Suite.

The default role of a new installation or upgrade of the HARMAN Media Suite is Media Suite Center. If the role of the HARMAN Media Suite is changed (from Media Suite Center to media node or from media node to HARMAN Media Suite Center), all configurations of the HARMAN Media Suite are set to default. You can change the server role from HARMAN Media Suite Center to media node through the console port.

Note: Cannot access the Media Suite by Web UI if the role is changed to Media Node

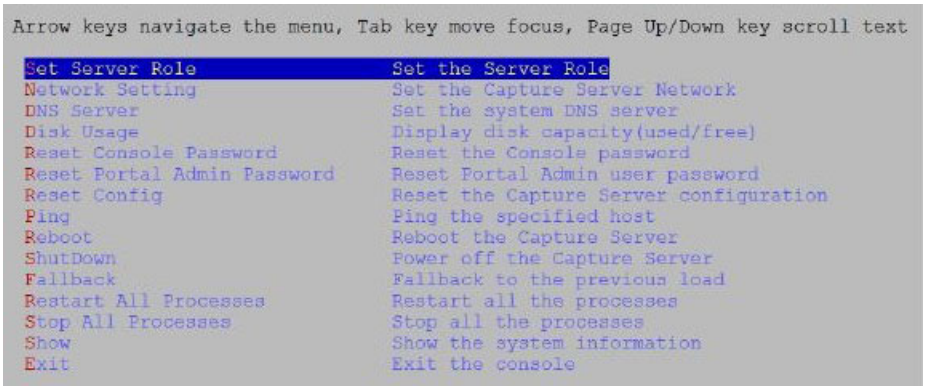
After the HARMAN Media Suite role is changed to Media Node, the Admin Portal is no longer accessible on that server, and administrator can manage the Media Node from admin portal on HARMAN Media Suite Center.

If Media Node disconnects from the HARMAN Media Suite Center for any failed network reason, you can access the Media Node through the console.

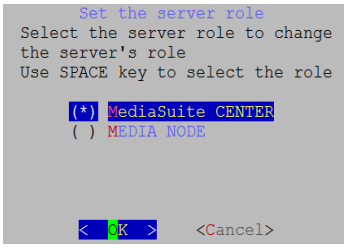
Procedure

1. (Appliance Edition) Connect a VGA monitor to the VGA interface of the HARMAN Media Suite system, and connect the USB keyboard to the USB interface of the HARMAN Media Suite system.
2. (Virtual Edition) Access through vSphere client console or SSH.
3. Open the console of your HARMAN Media Suite.

   The user name and initial password to access console are harman/harman. You must change the initial password when you log into the console first time.
4. Select **Set Server Role** by pressing the **Enter** key.



5. Select **Media Node**, and press **OK** to set the HARMAN Media Suite to Media Node.

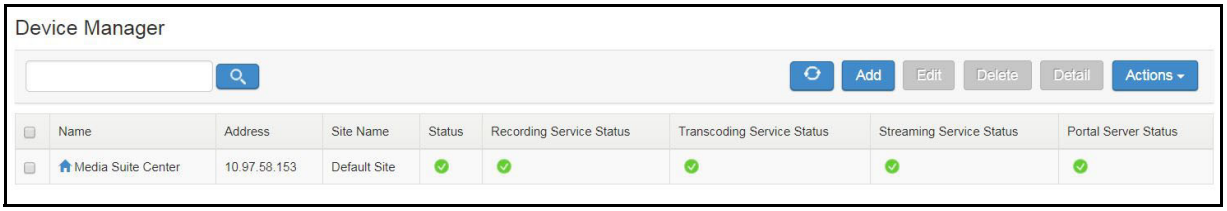


6. Set the HARMAN Media Suite Center IP address for Media Node, and click **OK**.
7. Click **Yes** to save the changes on the pop-up page.
8. Click **Yes** to reboot all services on the pop-up confirmation page.

   All the services reboot, and then log off.
9. Check the device setting of Media Node on the Admin Portal.
   1. In the address line, enter the Admin Portal IP address in this format: `http://<system IP address>/admin`, or `http://<FQDN>/admin`.

2 Enter the user name and password to log in to the system.

3 Go to **Device > Device Manager**.



4 Double-click a media node to check the device setting.

Related Links

Configuring a Device

You can add, edit, or delete devices from the HARMAN Media Suite admin portal.

In Scalability mode, one to fifty devices could be added in to cluster as Media Nodes.

Note: Open all required ports on the Firewall

Make sure all required TCP/UDP ports for HARMAN Media Suite Center and all Media Nodes are allowed on Firewall. For port list, refer to the *HARMAN Media Suite Release Notes.*

Add a Device in Virtual Edition

You can add a device to the HARMAN Media Suite admin portal using the Virtual Edition.

Once the settings are done, you have to reboot the system.

Procedure

1 Go to **Device > Device Manager**.

2 Click **Add**.

3 Configure the **Common** settings:

Common Settings

Parameter	Description
Device Name	Specify a unique name for the device name.
Register IP Address	Specify the IP address of the device.
Device Box Type	Specify the device box type as follows: • **HARDWARE**: for Appliance Edition • **VMWARE_VM**: for Virtual Edition • **AMAZON_AWS:** for a node in **AWS** cloud • **MS_AZURE:** for a node in **Azure** cloud **Note**: Only available when adding a new device.

4 Configure the **Network Setting.**

5 Click **Add** to add static routes.

Enter the following information for each route:

Set Route Parameters

Parameter	Descriptions
Destination	Specify the IP address of the destination network.
Gateway	Specify the IP address of the gateway to access the destination network.
Subnet Mask	Specify the subnet mask for the destination network.
Ethernet	Specify the Ethernet interface for the destination network.

6 Configure the **Media Storage** settings.

By default, HARMAN Media Suite, Virtual Edition, stores the files on a network file system if enabled to do so, or on a local hard disk. For the Appliance Edition, archives are saved on its local hard disk and the network file system could be configured.

7 Configure the **Service Setting**:

8 Click **Save** to apply your changes.

If more than one Media Node server is pointing to the HARMAN Media Suite Center, you can make the same changes to other Media Node servers.

9 Click **OK** to reboot the server.

10 Check the status of devices.

After the system reboots, the devices show a red status until the system is ready. Select the Refresh button to update the screen.

11 Create a Certificate Signing Request (CSR) and install a certificate.

After the settings is done, you have to re-boot the system for the settings to take effect.

Network Setting Parameters

Network setting parameters for device configuration.

Parameter	Description
Enable Networking Separation	Select this check box to route the management, streaming traffic, and video call traffic through LAN 1 and LAN 2 interfaces separately. Management network traffic, which includes Admin Portal and User Portal access, and steaming traffic, goes through LAN 1. Signaling network traffic, which includes signaling (H.323/SIP) and media traffic (RTP), goes through LAN 2. This offers higher security for the signaling data.
Network Settings (Networking Separation is disabled) Management Network (Networking Separation is enabled) Signaling Network (Networking Separation is enabled)	

Parameter	Description
Obtain an IP Address Automatically (DHCP)	If you select this radio button, HARMAN Media Suite obtains an IPv4 address automatically through DHCP. **Note:** Obtaining an IP address automatically is not recommended. For best results, assign a static IP to the HARMAN Media Suite.
Using the Following IP Address	• **IP Address:** the IP address of the system. • **Subnet Mask:** the subnet mask of the system. • **Default IPv4 Gateway:** the address of the interface used to access the IPv4 gateway.
Enable IPV6	Specify whether to enable IPv6 related functions.
Obtain an IP Address Automatically (IPV6)	Specify whether to obtain the IPv6 address automatically using Stateless Address Auto-configuration (SLAAC). **Note**: Obtaining an IP address automatically is not recommended. For best results, the system should be configured with a static IP address.
Using the Following IP Address (IPV6)	Select this option to manually configure a static IPv6 address: • **Link Local Address**: Specify an address for link local communication. Routers do not forward packets with link local addresses. • **Site Local Address**: Specify an address for site local communication. Routers do not forward packets with site local addresses. • **Global Address**: Specify one or several address for communication with external IPv6 networks. Separate several addresses with a comma (,). • **Default IPV6 Gateway:** Specify the address of the interface to use for accessing the IPv6 gateway.
Enable ICMP V6 DAD	Specify whether to enable Duplicate Address Detection (DAD) to ensure the IPv6 address set to the system is unique in the local network.
Enable ICMP Echo	Specify whether to allow the system to respond to an Internet Control Message Protocol (ICMP) echo request (Ping) sent from other devices in the network. In some high-security environments, you may need to disable this option to protect the system from Ping attacks.
MTU	Specify the Maximum Transmission Unit (MTU) size.
LAN Speed	Specify the speed or duplex modes for the LAN port. Select **Auto** to let the system set the speed automatically. **Note:** When setting the LAN port speed, contact your network administrator to ensure that the switch link rate matches the system port speed.
NAT Public (WAN) Address	Set the external IP address in a Network Address Translation (NAT) environment. NAT environments use private internal IP addresses for devices within the network, while using one external IP address to allow devices outside the LAN to access the HARMAN Media Suite Web Portal, view live streaming, or play back VoD.
General System Network Settings	
Host Name	Specify the host name of the system.

Parameter	Description
Domain	Specify the domain name of the system.
FQDN	Specify the FQDN for the HARMAN Media Suite. The FQDN must be correct and reachable. After configuring the FQDN, DNS must be configured for streaming service works well. In Scalability Mode, if https is enabled, FQDN should be configured for HARMAN Media Suite center and each Media Node. The FQDN of Media Node cannot be modified manually in AWS. If the HARMAN Media Suite integrates with Skype for Business, the FQDN must be configured.
Preferred DNS Server	The preferred DNS server address for the system to resolve domain names. If HARMAN Media Suite integrates with Skype for Business server, the DNS server information in Skype for Business server environment must be added to this field.
Alternate DNS Server	The alternate DNS server address for the system to resolve domain names.

Media Storage Setting for Virtual Edition

Media Storage Settings for Virtual Edition.

Parameter	Description
Media Storage Policy	Select the Media Storage Policy.
Local Storage Only	
Local Disk	Select one local disk from drop-down list for media storage.
Format new disk	Select the check box to format the new disk. **Note**: The format time depends on the size of the disk. A larger size would take a longer time.
Synchronize archives when storage setting changed	When this option is selected, the archive metadata in the new storage will sync up with the archive record in the system database.
Network Storage Only • If Network Storage Only is selected and the network storage is disabled or has an error, the HARMAN Media Suite cannot dial in and dial out. • HARMAN Media Suite supports NFS Versions 3 and 4. • For better NFS performance, make sure configure enough NFS CPU and memory resources.	
NFS Server Address	Enter an address of the NFS server.
NFS Storage Folder	Specify the folder path to the NFS storage. **Note:** Make sure the NFS server is set up. The NFS storage share folder must be different for all HARMAN Media Suite VE systems
Test	Test whether the NFS server is reachable.

Parameter	Description
Synchronize archives when storage setting changed	When this option is selected, the archives on the storage will be synced with the archive record in the system database, and can be viewed from either portal. The sync action takes effect after the system restarts. **Note**: This is a one-time operation. You need to check it again when you make storage change and need to sync up archives from the new storage.
Send warning email to the administrator when remaining NFS free disk space reaches (minimum 10 GB, maximum 500 GB) the configured threshold value	(For network storage) Set an NFS storage space threshold in the range of 10-500 GB (the default value is 10 GB). After the system reaches the threshold, the HARMAN Media Suite will send notifications to specified receivers.
Send warning email to the administrator when remaining local free disk space reaches (minimum 10 GB, maximum 500 GB) the configured threshold value	(For local storage) Set a local storage space threshold in the range of 10-500 GB (the default value is 10 GB). After the system reaches the threshold, the HARMAN Media Suite will send notifications to specified receivers.

Services Settings

Services settings parameters for device configuration.

Parameter	Description
Service Policy	Select **Enable All Services** to enable recording, transcoding, and streaming services, or select **Enable Streaming Service only** to enable streaming service only. • **Enable All Services**: the device supports all services, and provides recording, transcoding, and streaming functionality. • **Enable Streaming Service Only**: the device supports streaming service, and load balances the streaming service only. • **Enable Portal Service Only:** the device provides User Portal access only.

Parameter	Description
Enable Portal Server	Specify whether the device can provide User Portal service. If the service is enabled, customers can access the User Portal by server address or FQDN. Enabling additional portal servers on the Media Node helps to increase web session capacity (10,000 more per portal server), and may help to improve remote web portal access response speed by deploying portal server remotely. The option can only be disabled on Media Node.
Resource Policy	Specify the resource policy on the device. The option takes effect for the device with capacity more than 18/9. Specify the resource policy on the device to function as 18/9 model or 40/0 model if the hardware capacity of the device can meet 18/9 model's hardware specification. The option is only available when the **Enable All Services** is selected. • **Recording and Live Streaming**: the device supports both recording and live streaming. The capacity of device depends on the hardware configuration (CPU, RAM), for example, the device with 24 Core and 32G RAM supports up to 18/9. **Note**: In 40/0 mode, if **Recording and Live Streaming** is selected, only 18 recordings can be supported by system. • **Recording Only**: This feature allows the device to function as 40/0 maximum capacity to provide recording service without live streaming service. • The recording service distribution is based on the idle capability of each device in Scalability Mode.

Edit a Device

You can edit a device in the HARMAN Media Suite admin portal.

Procedure

1. Go to **Device** > **Device Manager**.
2. Select a specific device, and click **Edit**.
3. Configure the **Common** Settings and **Network Settings**.
4. Click **Add** to add static routes.
5. Enter information for each route.
6. Configure the **Media Storage** settings and **Service Settings**.
7. Click **Save** to apply your changes.

   If more than one media node server is pointing to the HARMAN Media Suite Center, you can make the same changes to other media node servers.
8. Click **OK** to reboot the server.
9. Check the status of the devices.

   After the system reboots, the devices show a red status until the system is ready. Select the **Refresh** button to update the screen.

   After the settings are done, you have to re-boot the system for the settings to take effect.

Reboot a Device

You can reboot a device from the HARMAN Media Suite admin portal.

Procedure

1. Go to **Device** > **Device Manager**.
2. Select devices which you want to reboot.
3. Click **Action** on the right corner.
4. Click **Reboot** to reboot the services on the selected device.

Shut down a Device

You can shut down the devices from the HARMAN Media Suite admin portal.

Procedure

1. Go to **Device** > **Device Manager**.
2. Select devices which you want to shut down.
3. Click **Action** on the right corner.
4. Click **Shutdown** to shut down the services on the selected device.

Reboot Device Services

You can reboot services from the HARMAN admin portal.

Procedure

1. Go to **Device** > **Device Manager**.
2. Select devices on which you want to reboot or shutdown services.
3. Click **Action** on the right corner.
4. Click to reboot the services on the selected device.

Shut Down Device Services

You can shut down device services from the HARMAN Media Suite admin portal.

Procedure

1. Go to **Device** > **Device Manager**.
2. Select devices on which you want to shutdown services.
3. Click **Action** on the right corner.
4. Click **Shutdown Service** to shut down the services on the selected device.

Enable User Portal Server

Media Node can work as portal server by enabling portal server on service setting, and the portal server can provide User Portal access service. Each portal server could support up to 10,000 web sessions, and the whole system supports up to 50,000 web sessions.

If multiple portal servers are configured in one cluster, each one can be accessed by its server address or FQDN, or admin can configure third party load balancer at front-end, to route the HTTP request to appropriate User Portal servers.

When you configure third party load balancer to access portal servers, enable **X-Forwarded-For** header to retain original IP address of Media Node.

Third party load balancer limitations

- Easy Capture does not support third party load balancer access, and can only log in to HARMAN Media Suite Center.
- Admin Portal cannot be accessed through third party load balancer IP address or FQDN, and only can be accessed through HARMAN Media Suite Center IP address or FQDN.
- Public API cannot be accessed through third party load balancer IP address or FQDN, and only can be accessed through HARMAN Media Suite Center IP address.
- The links generated from User Portal, including shared link, embedded link, event link, channel link, and QR link, use the HARMAN Media Suite Center IP address or FQDN in the link, but not the load balancer IP address or FQDN

Procedure

1. Go to **Device** > **Device Manager**.
2. Select devices on which you want to reboot or shutdown services.
3. Click **Edit**, and select **Service Setting** tab.
4. Select **Enable Portal Server**.

Migrating Media Data Among Devices

HARMAN Media Suite provides export and import media functions to migrate data among devices. This capability is useful for managing and protecting media data when adding, deleting, or replacing devices.

Export Media from the Devices

You can export media from the device.

Procedure

1. Go to **Device** > **Device Manager**.
2. Select the devices which you want to export media from.
3. Select **Action** > **Export Media**.

4 Configure the following settings for FTP server.

FTP Server Parameters

Parameter	Description
Server Address	Enter the IP address of the FTP server.
Port	Enter the port of the FTP server.
Media Backup Path	Specify the default FTP directory to save your media files.
User Name	Enter the account and password for login to the FTP server. **Note:** The registered FTP user should possess read-write permissions to user root directory.
Password	
Use Anonymous	When this is enabled, you can log in to the FTP server using anonymous account.
Test	Test whether the FTP configurations work.

5 Click **OK** to export the media from selected device to FTP server.

Import Media to Devices

You can import media to devices.

Procedure

1 Go to **Device** > **Device Manager**.
2 Select the devices to which you will import media.
3 Select **Action** > **Import Media**.
4 Configure the following settings for the FTP server.

FTP Server Settings

Setting	Description
Server Address	Enter the IP address of the FTP server.
Port	Enter the port of the FTP server.
Media Backup Path	Specify the default FTP directory to which you will save your media files.
User Name	Enter the account and password for login to the FTP server. **Note:** The registered FTP user should possess read-write permissions to the user root directory.
Password	
Use Anonymous	When this setting is enabled, you can log in to the FTP server using an anonymous account.
Test	Test whether the FTP configurations work.

5 Select **List Remote Folders**, and specify the folders that you will import from.
6 Click **OK**.

Configuring a Video Source

You can add, edit or delete video sources from the HRAMAN Media Suite admin portal.

Add a Video Source

You can add a device from the HARMAN Media Suite admin portal. Once the settings are done on the newly added device and saved, there is no need to reboot the system.

Procedure

1 Go to **Device** > **Video Sources**.
2 Select **Encoder** or **IP Camera** device type.
3 Click **Add**.
4 Configure the settings in the **Add Device** form: ***** indicates a mandatory field.

Form Settings

Parameter	Description
Device Type	Specify the current device type.
Device Name	Specify a unique name for the device.
URL (IP Camera only)	Specify a URL for the IP Camera device.
Username (IP Camera only)	Specify a username for the IP Camera device.
Password (IP Camera only)	Specify correct password for the username.
Streaming Protocol	Select a streaming protocol for the device. By default, RTMP is set for Encoder and RTSP for IP Camera.
Location	Specify a location for the device.
Status	Select a status for the device (Default: Active).

5 Click **OK**.

Set Recording Split Duration

For IP camera recording, you can split the duration of the recording.

The configured recording split duration is used to automatically split a recording. This is helpful to avoid long recordings, which will be difficult to analyze in case of any incident.

Recording Split Duration for IP Camera Events (Max: 12 hours, Min: 4 hours), default value is 12 hours.

To set the recording split duration, follow the procedure.

Procedure

1. Go to **Device** > **Video Sources**.
2. Select **IP Camera** in device type list.
3. From the **Recording Split Duration** drop-down list, select the appropriate value. (default value is 12 hours)
4. Click **OK** in the confirmation pop-up to save the changed value.

Edit a Video Source

You can edit a video source in the HARMAN Media Suite admin portal.

Procedure

1. Go to **Device** > **Video Sources**.
2. Select **Encoder** or **IP Camera** device type.
3. Select a specific device and click **Edit**.
4. Update the required fields in the device form.
5. Click **OK** to apply your changes.

Delete a Video Source

You can delete a video source in the HARMAN Media Suite admin portal.

Procedure

1. Go to **Device** > **Video Sources**.
2. Select **Encoder** or **IP Camera** device type. Select a specific device not in use. (A device can only be deleted when there is no associated active event for the selected device.)
3. Click the **Delete** button.
4. Click **OK** for Confirmation.

Configuring External Media Servers

You can now stream live meetings and on-demand meeting archives to leading third party media servers, such as Wowza, EdgeCast, Akamai, and CloudFront.

Note: Does not support IIS and Windows Media Server from v2.6

HARMAN Media Suite will not support IIS and Windows Media Server from v2.6. If you upgrade HARMAN Media Suite from previous version to v2.6, all configurations related to IIS and Windows Media Server will be cleaned.

HARMAN Media Suite treats external stream server (Wowza) and CDN (Akamai, CloudFront, and EdgeCast) differently:

- CDN can be used for global streaming, and can provide outside visiting.
- External stream servers are treated as internal visit the same as HARMAN Media Suite streaming server.

Configure the HARMAN Media Suite System for Working with Wowza Server

Configure a Wowza media server to work well with the HARMAN Media Suite as shown here.

Procedure

1. Click **WOWZA** under **Server**.
2. Click **Add**.
3. Configure the External Media Server settings, as shown here.

External Media Servers Parameters

Parameter	Description
Server Name	Specify the name of your **Wowza Media Server**.
Server Address	Specify the Wowza server IP address.
Server Port	Specifies the port that the HARMAN Media Suite system uses to send the encoded MP4 live streams to the external server. The Wowza Media Server default port is 1935. **Note**: Valid port values range from 1-65536. The port number must be the same as the one that is set in the corresponding external media server. If a firewall sits between the HARMAN Media Suite system and the external server, make sure that rules are set to allow the two-way communication between the HARMAN Media Suite system and the external server.

4. Specify whether to select **Enable Live**.

   If enabled, also configure the settings as follows:

Enable Live Streaming

Parameter	Description
Stream Protocol (for Wowza only)	Choose between **RTSP Steaming** and **RTMP Streaming**.
Application Name	Specify the name of the external media server's application to be used for the live streaming. **Note**: Contact the administrator of the external media server for the naming rule of the application name.
User Name	Specify the user name to access the external media server.
Password	Specify the password to access the external media server.
Test	Test whether the live streaming configurations are working.

5. Specify whether to stream video on demand (VoD) from this server.
   - Application Name: the name of the Wowza server application to be used for the VoD.It should be consistent with the Wowza server configuration. In this example, application name is VoD.

6 When **Enable Video on Demand** is selected, configure the following settings to transfer generated recordings to the Wowza server content directory:

Parameter	Description
FTP Address	Specify the IP address of the Wowza server.
FTP Port	Specify the port assigned to the Wowza server's FTP server. The default port is 21.
User Name	Specify your user name to access this FTP server.
Password	Specify your password to access this FTP server.
Default Path	Specify the default FTP directory to save your recordings. Use / to represent the root directory.
Enable SSL	Specify whether to enable SSL encryption for the communication between the HARMAN Media Suite system and the FTP server.
Test	Test whether the FTP configurations work.

7 Click **OK**.

You cannot create two external servers with the same Server type, IP, Port, and Application Name. To publish two bitrates to the same Wowza Server, create two instances of external server with different application name, and send each bitrate to one of two instances. This could be improved in later release by allowing multiple bitrates to be sent to the same external server instance. External latency time will be introduced when an external media server is configured compared with live streaming from the HARMAN Media Suite. The exact time varies depending on streaming protocol.

Configure AKAMAI CDN

You need to configure an AKAMAI media server and your HARMAN Media Suite to work with the server.

This is a charged function. You need an account to log in to the AKAMAI configuration page to get the needed parameters.

Procedure

1 Click **Server > AKAMAI**.

2 Click **Add**.

3 Configure the **External Media Server** settings.

Note: Contact AKAMAI account manager to change cross domain setting
The cross domain is enabled by default. If you want to disable the cross domain function, please contact your AKAMAI account manager.

External Media Servers Parameters

Parameter	Description
Configuration Name	The CONFIG NAME displayed on the AKAMAI configuration page under **PUBLISH > Manage Streams**.
Stream Name	Specify the stream name. The format should be `Name_1` where “Name” can be substituted with any stream name you choose.
Stream Number	The STREAM ID displayed on the AKAMAI configuration page under **PUBLISH > Manage Streams**.
Server Port	Specifies the port that the HARMAN Media Suite system uses to send the encoded MP4 live streams to the AKAMAI server. Valid port values range from 1-65,536. The port number must be the same as set in the corresponding external media server. Make sure port 80, port 443, and port 1935 are opened. **Note**: If a firewall sits between the HARMAN Media Suite system and the AKAMAI server, make sure that rules are set to allow the two-way communication between the HARMAN Media Suite system and the AKAMAI server.
Security Enabled	Enable secure token for AKAMAI streaming to prevent unauthenticated access by link sharing. After the security is enabled, user cannot play the video through other player by AKAMAI streaming URL. **Note**: the **Token Authentication** must be enabled in AKAMAI.
Key	Specified in **Active Password** on the AKAMAI configuration page.
Window	Specified the token expiration time. When the token expires, local player cannot play the streaming using the token. The default value is 300 seconds, and the minimum value is 10 seconds.
Entry Point	Specified on the AKAMAI configuration page under **PUBLISH > Manage Streams**.
HDS Playback URL	Specified on the AKAMAI configuration page under **PUBLISH > Manage Streams**. **Note:** After clicking **OK**, the HARMAN Media Suite substitute the [EVENT_ANGLE] with the **Stream Name** above automatically. If you copy the URL for other player, the [EVENT_ANGLE] must be changed to **Stream Name**.

Parameter	Description
HLS Playback URL	Specified on the AKAMAI configuration page under **PUBLISH > Manage Streams.** **Note:** After clicking **OK**, the HARMAN Media Suite substitute the [EVENT_ANGLE] with the **Stream Name** above automatically. If you copy the URL for other player, the [EVENT_ANGLE] must be changed to **Stream Name**.
User Name	Specify your entry point user name to access the AKAMAI server.
Password	Specify your entry point password to access the AKAMAI server.

4 Click **OK**

Note: AKAMAI is a charged function
This is a charged function. You need an account to log in to the AKAMAI configuration page to get the needed parameters.

Configure EdgeCast CDN

You need to configure an EdgeCast media server and your HARMAN Media Suite to work with the server.

Configure EdgeCast Media Server

You can configure EdgeCast media server parameters for working with HARMAN Media Suite.

Procedure

1 Go to **Server > EdgeCast**.
2 Click **Add**.
3 Configure the Edgecast basic settings, as shown next:

External Media Servers Parameters

Parameter	Description
Configuration Name	Specify the configuration name of the external server.
Server Port	The port that the HARMAN Media Suite system uses to send the encoded MP4 live streams to the EdgeCast server. The value is 1935.
Live Streaming	
Publishing Point	Specify a publishing point for EdgeCast.
HDS Player URL	Specified on the EdgeCast configuration page.
iOS Player URL	Specified on the EdgeCast configuration page.

Parameter	Description
Stream Name	Specify the stream name.
Authentication Key	Specified on the EdgeCast configuration page: **Flash > Live Auth > Global Key**.

4 Click **OK**, and HARMAN Media Suite substitutes the **Stream Name** and **Authentication Key** to replace <streamName> and <Live Authentication Key> in the publishing point URL.

Note: EdgeCast is a charged function
This is a charged function, so you need an account to log in to the EdgeCast configuration page for the necessary parameters.

Configure CloudFront CDN

CloudFront is a content delivery service provided by Amazon, which speeds up distribution of static and dynamic content to end user.

The HARMAN Media Suite integration with CloudFront now only support live streaming integration, and requires must work with Wowza instance on AWS to stream live.

You need to configure a CloudFront media server, a Wowza server on AWS and your HARMAN Media Suite to work together.

Create a Wowza instance in AWS

You can create a Wowza instance in AWS.

Procedure

1 Log in the Amazon Web Service on https://aws.amazon.com/.
2 Select **EC2** under **Compute.**
3 Click **Launch Instance** under **Create Instance** to launch HARMAN Media Suite AMI.
4 Select Wowza AMI from AWS Marketplace, and click **Select** to launch a Wowza instance. The Wowza instance works with CloudFront to stream live from HARMAN Media Suite.

   To launch an instance, refer to AWS Support Center.
5 Access Wowza instance to create an Application Name. For more information about Wowza instance, refer to Wowza on AWS.

Create a CloudFront in AWS

You can create a CloudFront in AWS.

Procedure

1 Create a CloudFront in AWS. For more information, refer to Live HTTP Streaming Using Wowza Streaming Engine.

Configure CloudFront Media Server Instance on HARMAN Media Suite

You can configure a CloudFront Media Server instance on the HARMAN Media Suite.

CloudFront is a charged function and need Pro license, so you need an account to log in to the Amazon configuration page for the necessary parameters.

Procedure

1. Go to **Server > CloudFront**.
2. Click **Add**.
3. Configure the CloudFront basic settings, as shown next:

External Media Servers Parameters

Parameter	Description
Server Name	Specify the CloudFront media server instance name.
Server Address	The Elastic IP of the Wowza instance.
Server Port	Specify the port that the HARMAN Media Suite system uses to send the encoded MP4 live streams to the Wowza. The default port is 1935. Valid port values range from 1-65536. The port number must be the same as the one that is set in the corresponding Wowza on AWS. If a firewall sits between the HARMAN Media Suite system and the external server, make sure that rules are set to allow the two-way communication between the HARMAN Media Suite system and the external server.
Live Streaming	
Streaming Protocol	Choose between **RTSP Steaming** and **RTMP Streaming**.
Application Name	Specify the name of the Wowza application to be used for the live streaming. Get Wowza application name from Wowza instance.
Publishing Point	Specify a publishing point for CloudFront.
Distribution Domain Name	The Distribution Domain Name displayed on the CloudFront Distributions page under **AWS** > **CloudFront**.
User Name	The user name of the Wowza server which connects to the CloudFront.
Password	The password to access the Wowza server which connects to the CloudFront.

4. Click **OK.**

Configure Publish Point

Dynamic publish point and static publish point are configured in a distribution template.

If one static publish point is configured in the distribution template, the template is the static template and can be used for only one live event.

User and Group Management

Topics:

You can manage users and groups in the HARMAN Media Suite system.

You can assign roles to existing users, create new local users, and edit their information.

Working with Users and Roles

There are several way to manage users and groups in the HARMAN Media Suite system which are explained here.

Types of Users

The HARMAN Media Suite supports two types of users.

- Enterprise Users that come directly from the Active Directory (AD) users.
- Local Users that are local to the management system. These users are added manually to the system.

Local Users

When you manually add local users, the HARMAN Media Suite manages all user information and associations.

At a minimum, when you manually add users, you must enter a user's Username, Full Name, Email Address, and Password. After you enter the minimum information, the HARMAN Media Suite automatically assigns local user the role you selected from Role.

Enterprise Users

When the HARMAN Media Suite is integrated with an Enterprise Directory, the user information is pulled from the Enterprise Directory.

User Roles

Users who are defined in the HARMAN Media Suite system can log in to the system admin portal to complete authorized operations.

The system supports two user roles to log in to the admin portal:

- Auditor: Audit and manages system logs and sets personal information.

- Administrator: Performs most of the operations, and can view and configure all pages.

User Permissions through the Admin Portal

You can log in to the admin portal as an administrator or an auditor.

The following table explains user permissions.

Content	Auditor	Administrator	User
Accessible information	System logs	All pages	Cannot access Admin Portal.
Operations permissions	View, download, and delete system logs	View, edit, and delete archives View and download system logs	Cannot access Admin Portal

Managing Users

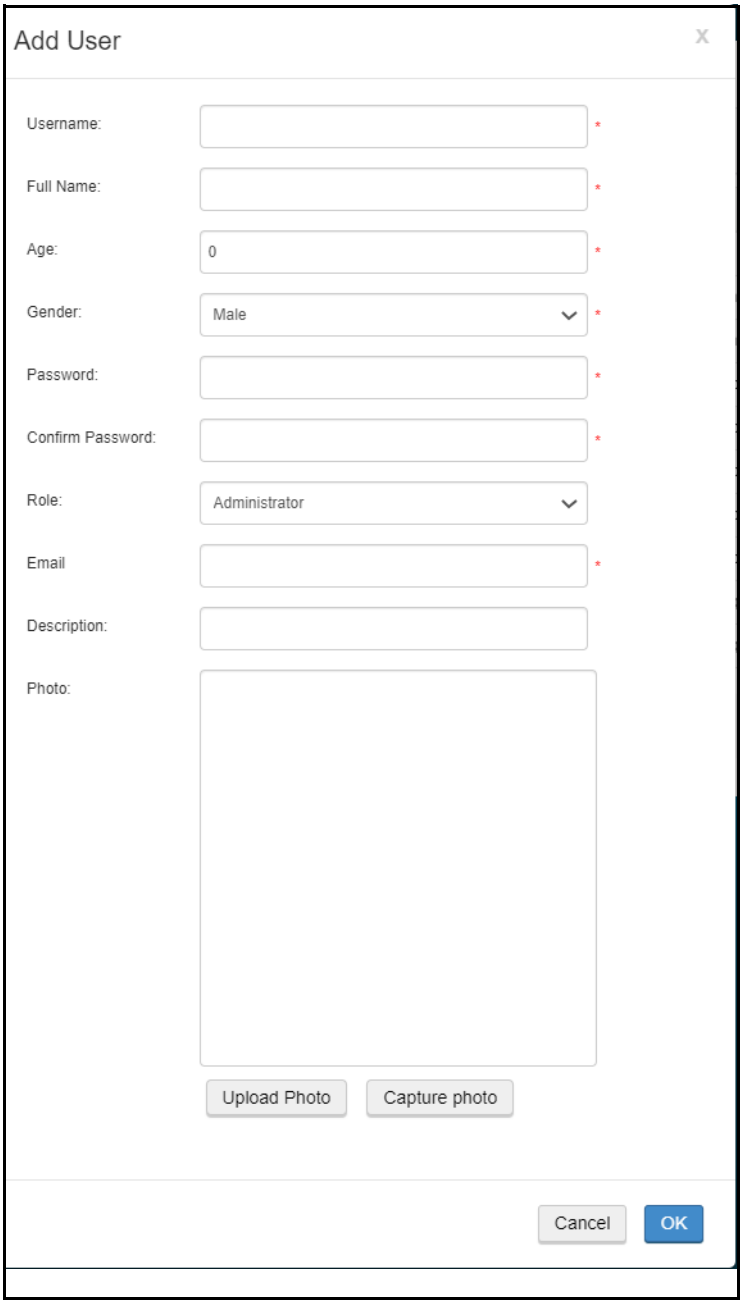
You can manage users in the HARMAN Media Suite system.

Add a New Local User

You can add a local user to the system.

Procedure

1. Go to **User > Users**.
2. Click **Add**.
3. Configure the settings.


Add User
x
Username:
Full Name:
Age:
0
Gender:
Male
Password:
Confirm Password:
Role:
Administrator
Email
Description:
Photo:
Upload Photo
Capture photo
Cancel
OK

Adding a User

Setting	Description
Username	Specify the user name used for web login. The user name must be unique with a length of 1-128 characters, and consist of alphanumeric or "_" symbol characters. Once created, the user ID cannot be modified.
Full Name	Specify the user's full name.
Age	Specify the user's age.
Gender	Select user's gender from the drop box.
Password	Specify the login password.
Confirm Password	Specify the confirmed password, which must be identical to the login password.
Role	User roles: **Administrator**, **Auditor,** or **User**. Different roles determine the user operation permissions after logging in to the pages.
Email	Specify the user’s email address.
Description	Specify additional related information.
Photo	The user's photo of 75x75 pixels, which has clear frontal face of the user for better search performance. If the photo is already available, use the **Upload Photo** option. Or use the **Capture Photo** option to start webcam and capture the photo.

4 Click **OK**.

Modify User Information

You can edit the user information.

Procedure

1 Go to **User > Users**.
2 Select the user entry you want to edit.
3 Click **Edit**.
4 Enter the user information, and then click **OK**.

Unlock a user

You can lock and unlock a user.

Procedure

1 Go to **User > Users**.
2 Select the user entry you want to edit.
3 Click **Edit**.

4 Change the status of the user from **Status** drop-down list. If the user is locked, you can change the status from **Locked** to **Active** for unlocking.

Modify Local User Password

You can modify the password for local users only.

Procedure

1 Go to **User > Users**.
2 Select the user entry you want to modify.
3 Click **Reset Password**.
4 Enter the new password and confirm password, then click **OK**.

After the password is changed by the administrator, the user is required to change the password after logging in to the system using that password for the first time.

Delete a User

You can delete a user.

Procedure

1 Go to **User > Users**.
2 Select the user entry you want to delete.
3 Click **Delete**.

Managing the Role of an Enterprise Directory User

The administrator can assign administrator role to Enterprise Directory User.

Assign Role to Enterprise Directory User

You can assign administrator role to Enterprise Directory user.

Procedure

1 Go to **User > Users**.
2 Select **AD Users** from down-drop list.
3 Select **Grant Permission**.
4 Enter the full or part of the AD user name in **User Name**.
5 Click **Search** to find the AD user, and select the user you want to grant the role from **User ID** down-drop list.

   After selecting the AD user, system shows the full name, domain, Email, and description of user for double check.
6 Select **Administrator** from the **Role** down-drop list to grant a role to the AD user.

7 Click **OK**.

The Enterprise Directory users who are granted permission cannot be backed up when you back up the system configuration. You have to back up Grant Permission Enterprise Directory users manually before backing up system configuration

Change the Role of Enterprise Directory User

You can change the role of the Enterprise Directory users.

Procedure

1 Go to **User > Users**.
2 Select **AD Users** from down-drop list.
3 Select a AD user, and select **Change Permission**.
4 Select **Administrator** from the **Role** down-drop list to change the role of the AD user.
5 Click **OK**.

Delete the Role of Enterprise Directory User

You can delete the role of an Enterprise Directory user.

Procedure

1 Go to **User > Users**.
2 Select **AD Users** from down-drop list.
3 Select a AD user, and select **Clean Permission**.
4 Click **OK** on the pop-up confirmation page.

Log In to the Admin Portal

You can log in to the admin portal.

Procedure

1 In the address line, enter the system IP address in this format:

```
http://<system IP address>/admin , or http://<FQDN>/admin .
```

The HARMAN Media Suite supports http and https to log in to the system. When an IPv6 address is used, use the following format:

```
http://[IPv6]/admin
```

2 Enter your user name and password to log in to the system (The initial user name and password are `admin/Harman12#$)`.

Working with Groups

Groups can be used in the user portal for assigning viewers and contributors to a Channel.

You can create user groups and set permissions for groups.

A default group, named all-users, is built into the system. It includes all the users defined in the HARMAN Media Suite system. The all-users group cannot be modified or deleted. Administrators can define a new group, and modify or delete existing groups.

View User Groups

You can view user groups.

Procedure

1. Go to **User > Groups**.
2. Filter by **Local Groups** or **AD Groups.**

Create a New User Group

You can create a new user group.

The local group created here can only be added with local user only, and enterprise users can only be added to enterprise user group created in Active Directory.

To create a new user group:

1. Go to **User > Groups**.
2. Click **Add**.
3. Specify a unique name for the group.

   You can enter associated descriptions if necessary.
4. Click **Group Members**.
5. Select users to add to the group, and then click **Add**.

   To delete an item, select it and click **Remove**.

Modify an Existing Group

You can modify an existing group.

Procedure

1. Go to **User** > **Groups**.
2. Select the group entry you want to edit.
3. Click **Edit**.

Delete an Existing Group

You can delete an existing group.

Procedure

1. Go to **User** > **Groups**.
2. Select the group entry you want to delete.
3. Click **Delete**.

Record and Playback

Topics:

Set Recording Parameters

You can configure supplementary recording settings.

The system call setting will be applied as the default value to all calls in the system. If there is a difference in the recording templates, the setting of the recording template will take precedence.

Procedure

1. Go to Configuration > Call Settings.
2. Configure the recording settings, as shown next:

Setting	Description
Allow recording when live streaming can not be created.	If this option is selected, the call can connect and the system automatically records the meeting to the hard disk when there are insufficient resources available to live stream a meeting. You cannot continue viewing the live in real time through the web. However, you can play back the video upon the completion of recording and format conversion. If this option is not selected, the system rejects all calls that have live streaming enabled when there are no live streaming resources. The option takes effect on the call dialed from admin portal.
Key Frame interval	Specify the fast forward and backward intervals when playing back recorded files on an endpoint. For example, if the interval is set to one minute, the system inserts an index marker every minute when recording. When you press **Fast Forward** using Far End Camera Control (FECC) or DTMF, the video playback jumps to the nearest index marker from the current location. Shorter intervals result in larger archive.
Indication Tone	Indicates that recording is ongoing, and typically the tone is a very short beep with intervals between beeps, measured in seconds.

Setting	Description
Media Encryption	If the HARMAN Media Suite is licensed for call encryption, this option specifies how Advanced Encryption Standard (AES) encryption is enabled for H.323 and SIP calls: • **Required For All Calls**: Enable the AES encryption for all H.323 and SIP calls, including video and audio-only calls. This option requires the device to connect to the AES enabled system, otherwise, the connection cannot be set up. • **When Available**: Enable the AES encryption when the peer device enables the AES option, and vice versa. • **Off**: Disable the AES encryption. This feature doesn't function in maximum security mode. This is the system level configuration, and you can set media encryption for specific recording template. Note: Encryption of SIP Media requires the encryption of SIP signaling- TLS Transport Layer must be used.
Support AES 256-Bits key for encryption	If the HARMAN Media Suite is licensed for call encryption, this option specifies whether to enable the 256-bits key for AES encryption on media streams. If not selected, the AES uses the 128-bit key for encryption on media streams by default.
Max Call Length (for streaming only call)	The maximum call length for streaming-only calls. The value is 8 hours by default. Note: There is no limitation to this option.
Max Call Length	The maximum call length for recording calls. The value is 16 hours by default. Valid call length ranges from 1 to 16 hours.
Enable all IVR notifications	When the IVR service at the system level is enabled, the default remaining time to play IVR is 10 minutes.
Enable Global Quickcode Playback PIN	Enable quickcode playback PIN at the system level.Note: If a PIN code is set under the archive properties, the individual PIN code will override that set at the system level.
NAT Enable	Select check box to enable NAT.
NAT Keep Alive Interval	Specify the NAT timeout interval.

3 Click **OK**.

Working with Templates

A template is used to define a set of basic recording parameters, such as call rate of recording, video quality, whether to live stream, and streaming rate.

All Virtual Recording Rooms (VRR) are created based on templates. Changing the parameters of a template may change the corresponding recording policies of the VRR using that template.

Working with Recording Templates

In this section you'll learn how to configure recording templates, including how to view, define, edit, or delete them.

View a Recording Template

You can view a recording template.

Procedure

- Go to **Template > Recording Templates**.

Define a Recording Template

You can define a recording template.

Procedure

1. Go to **Template > Recording Templates**.
2. Click **Add**.
3. Configure the recording template settings, as shown next:

Recording Template

Parameter	Description
Template Name	Specify a unique name to identify this template.
Enable Live Streaming	Enable live streaming for the calls that use this template.
Disable Recording	This setting is available when **Enable Live Streaming** is selected. The call will be live streamed only, without recording.
Enable PIN	Specify whether to enable PIN code protection for the live streams. If a PIN code is set, you must enter the correct PIN code to play the live streams for the calls that use this VRR. After this option is selected, you must enter a PIN code consisting of 1-16 digits in **PIN Code**.
Call	
Audio Only	Select this check box to define the recording for the call with this template, which has only audio capability, no matter the call rate negotiated.
Max Call Rate	Specify the maximum bandwidth that can be used by an endpoint or MCU to connect to the HARMAN Media Suite system for recording and live streaming.
Max Resolution	Specify the maximum resolution of people video that can be used to connect to the HARMAN Media Suite system for recording and live streaming.
Enable LPR	Once this function is selected, in case of packet loss during network transmission, it can effectively improve the decreased video quality caused by packet loss.
Indication Tone	Indicate that recording is ongoing, and typically the tone is a very short beep with intervals between beeps, measured in seconds. This is enabled by default.

Parameter	Description
Media Encryption Type	If the HARMAN Media Suite is licensed for call encryption, this option specifies how Advanced Encryption Standard (AES) encryption is enabled and SIP connections: • **Required For All Calls:** Enables the AES encryption for all H.323 and SIP calls, including video and audio only calls. This option requires the device to connect the system with AES enabled, otherwise, the connection cannot be set up. • **When Available:** Both encrypted and non-encrypted undefined participants can connect to the same conferences, where encryption is the preferred setting. • **Off:** Disable the AES encryption. This option requires the device to connect the system without AES enabled, otherwise, the connection cannot be set up. Media Encryption Type is the template level configuration, and must consist with the system level configuration under Set Recording Parameters: • The default value is the setting of **Media Encryption** under Set Recording Parameters. • If the system level Media Encryption is set to **Required For All Calls**, only the **Required For All Calls** can be selected. • If the system level Media Encryption is set to **When Available**, the **Required For All Calls** and **When Available** can be selected. • If the system level Media Encryption is set to **Off**, the **Required For All Calls**, **When Available,** and **Off** can be selected. **Note**: The Media Encryption Type change is applied to new created recording template, and does not impact the existing recording template.
Max Call Length	Specifies the maximum call length for recording or live streaming calls. The default option is **Auto** (When selected, the max call length setting will be the same as configured under **Configuration > Call Settings**). Note: The template value set here will override the system value set under **Configuration > Call Settings** on the Admin Portal.
Conference Layout (Collaboration Server (RMX) 8.4 or higher)	Specify the people layout received and recorded from the MCU. The **1x1** and **1x2** layout may give focus on the speaker of the conference in the recording. • **Auto:** Automatic layout according to conference settings at the Collaboration Server (RMX) side to the recording server. • **1x1:** Single view to recording server. • **1x2:** Dual view to recording server.
Archiving	
Start Recording Immediately	If this option is selected, the system immediately starts recording with this recording template. If deselected, you may need to manually start recording through the Admin Portal or the TV UI. **Note:** For H.323 call to Collaboration Server (RMX), if the option is selected, the IVR “conference is being recorded” cannot be promoted after starting a recording.
Archive Name Prefix	Specify the prefix of the output media archive name.
Live Streaming (MP4) Not available for audio-only live streaming.	

Parameter	Description
Enable H.264 High Profile for Live Streaming	Select this check box to enable the use of H.264 High Profile.
Primary Streaming Rate (Kbps)	The default value is 1024 kbps. Once the streaming rate is set, you can define a name for this streaming.
Secondary Streaming Rate (Kbps)	The default value is **Off**. After the streaming rate is set, you can define a name for this streaming.
Layout	Specify the layout for displaying people and content videos when transcoding the dual stream. Users can choose from the following layouts: • **Single window with small content (People 75%; Content 25%):** Displays dual stream in one window, of which 75% is people video and 25% content video. • **Single window with medium content in right (People 50%; Content 50%)** Displays dual stream in one window, of which 50% is people video and 50% content video on the right side. • **Single window with medium content in left (People 50%; Content 50%)** Displays dual stream in one window, of which 50% is people video and 50% content video on the left side. • **Single window with large content (People 25%; Content 75%):** Displays dual stream in one window, of which 25% is people video and 75% content video. • **Single window with people only (content not shown):** Displays people video only in one window, with no content. • **Single window with people or content (when content active):** When people and content videos coexist, content video takes priority, people video displays only when content is absent. • **Dual window for content (when inactive content, it is black):** The stream supports dual windows, one for people video, the other for content video, black screen displays when content is absent. **Note:** Dual window for content is not supported for live streaming to external media servers.
Live Streaming (WMV) **Note:** WMV is only available in standalone mode and cannot be supported in scalability mode. Not available for audio-only live streaming.	
Primary Streaming Rate (Kbps)	The default value is **Off**. Once the streaming rate is set, you can define a name for this streaming.

Parameter	Description
Secondary Streaming Rate (Kbps)	The default value is **Off**. Once the streaming rate is set, you can define a name for this streaming.
Layout	Specify the layout for displaying people and content videos when transcoding dual stream. Users can choose from the following layouts: • **Single window with small content (People 75%; Content 25%):** Displays dual stream in one window, of which 75% is people video and 25% content video. • **Single window with medium content in right (People 50%; Content 50%)** Displays dual stream in one window, of which 50% is people video and 50% content video. • **Single window with medium content in left (People 50%; Content 50%)** Displays dual stream in one window, of which 50% is people video and 50% content video. • **Single window with large content (People 25%; Content 75%):** Displays dual stream in one window, of which 25% is people video and 75% content video. • **Single window with people only (content not shown):** Displays people video only in one window, with no content. • **Single window with people or content (when content active):** When people and content videos coexist, content video takes priority, people video displays only when content is absent. • **Dual window for content (when inactive content, it is black):** The stream supports dual windows, one for people video, the other for content video, black screen displays when content is absent. **Note**: HARMAN Media Suite Player does not support Dual Windows for WMV video.

4 Click **OK**.

You can click **Save As** to clone a new template with the same settings.

Edit a Recording Template

You can edit an existing recording template.

Procedure

1 Go to **Template > Recording Templates.**
2 Click the recording template you want to change.
3 Click **Edit** or **Delete**.

Delete a Recording Template

You can delete an existing template.

Procedure

1 Go to **Template** > **Recording Templates**.

2 Click the recording template you want to delete.3.
3 Click **Delete**.

Maximum Call Length

Maximum call length is used to restrict the call length for recording and streaming calls for the following reasons:

- When recording a meeting, the recording call may be endless (to Collaboration Server (RMX) for example) and thus flood the disk with unused data.
- A recording longer than 16 hours is difficult to be transcoded offline.
- An endless streaming only session will cost transcoding resource occupancies.

Set max call length for recording and streaming calls

You can set max call length for recording and streaming calls.

Procedure

1 Go to **Template > Recording Templates**.
2 Select the recording template you want to change.
3 Click **Edit**.
4 Choose a value from the **Max Call Length** drop-down list.
   - The max call length is a guard timer used to automatically stop recording and to disconnect from the recording client when timer times out. This is helpful to avoid flooding the disk if the recording server fails to end the call after the recording event.
   - For a recording call (with or without live streaming), the default setting is 2 hours, range is 1-16 hours. For live streaming only calls, the default setting is 8 hours and there is no limitation to the max range.
   - When a call is approaching the max call length, an IVR message will be sent to the user as a reminder.

Set max call length for streaming-only calls

You can set max call length for streaming-only calls.

Procedure

1 Go to **Template > Recording Templates.**
2 Click the recording template you want to change.
3 Click **Edit**.
4 Select **Disable Recording**.
5 Clear **Auto under Max Call Length**.
6 Enter your desired value.

   Input positive numbers, and the value 0 indicates no limitations to this option.

Working with Transcoding Templates

You can configure view, define, edit, or delete a transcoding template.

You can also learn how to replicate transcoding templates for external media servers.

Define a Transcoding Template

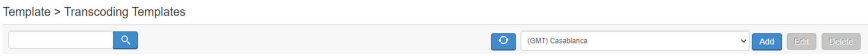
You can define a transcoding template.

Procedure

1. Go to **Template > Transcoding Templates**.
2. Click **Add**.
3. Configure the transcoding template settings, as shown next:

Transcoding Template

Parameter	Description
Template Name	Specify a unique name to identify this template.
Media Type	Specify the output media file format.
Video	
Bit Rate	Specify the output media file bitrate.
Video Type	The video protocol used by the archive.
Frame Rate	Specify the media frame rate.
Max Resolution	Specify the maximum transcoding resolution.
Aspect Ratio	Specify the aspect ratio of the output media file.
Layout	Specify the layout for displaying people and content videos when transcoding dual stream. Users can choose from the following layouts: • **Single window with small content (people 75%; content 25%):** Displays dual stream in one window, of which 75% is people video and 25% content video. • **Single window with medium content in right (People 50%; Content 50%)** Displays dual stream in one window, of which 50% is people video and 50% content video. • **Single window with medium content in left (People 50%; Content 50%)** Displays dual stream in one window, of which 50% is people video and 50% content video. • **Single window with large content (people 25%; content 75%):** Displays dual stream in one window, of which 25% is people video and 75% content video. • **Single window with people only (content not shown):** Displays people video only in one window with no content. • **Single window with people or content (when content active):** When people and content videos coexist, content video takes priority, people video displays only when content is absent. • **Dual window for content (when inactive content, it is black):** The stream supports dual windows on Windows Media Player, one for people video, the other for content video, black screen displays when content is absent.

Parameter	Description
Enable VoD Timecode Watermarking	Specify whether to enable Timecode (GMT) Watermarking functionality for VoD. **Note**: For Watermarking function, you can change the Time Zone (GMT) by selecting it from the drop-down in **Template > Transcoding Templates**. 
Snapshot	
Snapshot Enable	Specify whether to generate thumbnails for transcoded media files. If you want to enable choosing archive cover from thumbnails on User Portal, the archive transcoding template must enable snapshot.
Remove Duplicate Thumbnail	Delete the duplicate snapshots that resulted from the thumbnail generation process.
Enable Auto Snapshot During Entire Call	When enabled, snapshots can be generated automatically throughout the entire call.
Start Time	Select the start time for the automatic thumbnail generation. Only available when **Enable Auto Snapshot During Entire Call** is not selected.
End Time	Select the end time for the automatic thumbnail generation. Only available when **Enable Auto Snapshot During Entire Call** is not selected.
Interval (seconds)	Set the snapshot interval, measured in second. Only available when **Enable Auto Snapshot During Entire Call** is selected.
Transfer to Media Server	Select the media servers you want to transfer media files to after transcoding in the **Available Server** list.The media server includes HARMAN Media Suite Center, Media Node, and the an external media server. The MP4 format media file can be transferred to WOWZA server. For external media server configuration details, refer to Appendix B – Configure Wowza Media Server.

4 Click **OK**.

You can click **Save As** to clone a new template with the same settings.

Preconfigured Templates for iOS and Android

You can find some preconfigured templates for iOS and Android, as shown next:

You can find some preconfigured templates for iOS and Android, as shown next:

Preconfigured Templates for iOS

Template Name	Resolution	Frame Rate	Bitrate	Aspect Ratio	Device	Profile
Iphone_M_2	640*480	30	1,280	4:3	iPhone4 & above	Baseline
Iphone_S_2	480*360	15	464	4:3	iPhone4 & above	Baseline
Ipad_L	1024*768	30	1,024	16:9	iPad 2, iPad mini	Baseline
Iphone_M_1	640*360	30	664	16:9	iPhone4 & above	Baseline
Ipad_H	1920*1080	30	1,728	16:9	New iPad, iPad Retina Display	High Profile
Iphone_S_1	480*270	15	464	16:9	iPhone4 & above	Baseline

Preconfigured Templates for Android

Template Name	Resolution	Frame Rate	Bitrate (Kbps)	Profile
SD_H	480*360	30	512	Baseline
SD_L	176*144	12	128	Baseline
HD	1280*720	30	2048	Baseline

View a Transcoding Template

You can view a transcoding template.

Procedure

- Go to **Template > Transcoding Templates**.

Configure a Transcoding Template for the WOWZA Media Server

You can configure a transcoding template for the WOWZA media server.

Procedure

1. Go to **Template > Transcoding Templates**.

2 Click **Add.**
3 Select **MP4** for **Media Type**.
4 Select the WOWZA media server you configured in the **Transfer to Media Server** field.

Edit or delete a transcoding template

You can edit or delete an existing transcoding template.

To edit or delete a transcoding template:

1 Go to **Template > Transcoding Templates.**
2 Select the transcoding template you want to change or delete.
3 Click **Edit** or **Delete**.

Working with Virtual Recording Rooms (VRRs)

A VRR defines recording parameters. You can create a VRR basing on recording templates. A VRR is identified by digits, and you can directly start recording using a specified VRR by adding the VRR number to the dial-in number.

A default VRR, named ***Default VRR***, is built into the system. When an endpoint or MCU tries to connect by dialing the HARMAN Media Suite without a VRR number specified, default VRR parameters are used. You can modify the default VRR but cannot delete it.

Define a VRR

You can define a VRR.

Procedure

1 Go to **Template > VRRs**.
2 Click **Add**.
3 Configure the VRR settings, as shown next.

VRR Settings

Parameter	Description
VRR Name	Specify a unique name to identify the VRR. You can also use the default name generated by the system.
VRR Number	Specify a number to identify the VRR. You can directly dial the VRR to record by adding the VRR number when dialing the HARMAN Media Suite system. The number you enter must be unique and comprised of 4-8 digits. You can also use the number automatically generated by the system. **Note**: The initial digit of the VRR number cannot be zero.

Parameter	Description
Enable Register to Lync	Specify whether register VRR to Skype for Business server. When user dials out from Skype for Business to the HARMAN Media Suite, user can choose different recording template by invite different registered user to Skype for Business meeting after configuring VRR and integrating the Skype for Business user with VRR.
Lync Register Name	Specify a Skype for Business user combined with the VRR.
Description	If necessary, you can enter additional VRR information, such as the owner and usage, in order to improve identification and classification management when there are many VRRs.
Recording Template	Specify the recording template. The template defines the basic recording link parameters.
Distribution Template	Specify the distribution template. The template defines the live streaming distribution rule and player policy.
Transcoding Template	After recording is done, the system will do offline transcoding according to the transcoding templates configured here. Multiple offline transcoding outputs are allowed. Only qualified transcoding templates will apply. If the template parameters are higher than the recorded raw parameters, then the template will be ignored. For example, if recording raw resolution (e.g. 4CIF) is less than the transcoding template (e.g. 720p), then this transcoding template will be ignored. **Note**: If the recording template disable the live streaming, the transcoding template is required for playing back video correctly.
VRR Auto Publish Only	If **Yes** is selected, this VRR only can be used for VRR auto publish and is not shown in the VRR list when creating a recording or live event. **No** is the default setting and cannot be changed in **Default VRR**.
Email Address (separated by ‘,’)	Once the live streaming is started or the VRR recorded video has completed its format conversion and is ready for viewing, the system sends an email message to the address set here.

4 Click **OK**.

You can click **Save As** to clone a VRR with the same settings.

Limitations on recording Skype for Business meeting

- Skype for Business server and HARMAN Media Suite recording across Firewall/NAT is not supported.
- HARMAN Media Suite supports recording for Microsoft AVMCU conference, which is created by clicking **Meet Now**. However, one Skype for Business client calling the HARMAN Media Suite directly to record the meeting is not supported.
- HARMAN Media Suite does not support XMPP, so the registration status of HARMAN Media Suite or the VRR on Skype for Business client is always offline.
- Only RTV (AVC) is supported.

- In a Skype for Business meeting, if the active speaker is on-hold for 20 seconds and no other participants promote to active speaker, and no Remote Desktop Protocol (RDP) content changes, HARMAN Media Suite disconnects automatically. This is caused by HARMAN Media Suite protection progress; when there is no audio, video, and content received for 20 seconds, HARMAN Media Suite disconnects the call to reclaim the resource.
- In a live streaming of Skype for Business meeting which is audio-only, if all participants are mute or no one speak for 30 seconds, the live streaming will be disconnected due to no audio packet between Skype for Business server and HARMAN Media Suite.

Edit or delete a VRR

You can edit or delete an existing VRR.

Procedure

1. Go to **Template > VRRs**.
2. Click the VRR entry you want to edit or delete.
3. Click **Edit** or **Delete**.

Archives Playback Selection

If more than one transcoding template is selected in VRR, when play back the archive, system chooses an archive based on the following rules:

- For IE browser, system chooses archive in WMV format to play.
- For other browsers, if you use the HARMAN Media Suite Player, system first chooses dual-window archive to play. If you use other player not the HARMAN Media Suite Player, system chooses single-window archive to play. The rules for choosing archive in more than one single-window archives:
  1. System first chooses the archive in mp4 format with1,024k bitrate and 720p30 resolution.
  2. If no archive can meet the first criteria, system chooses archive with quality lower than the first criteria, but the closest one to play.
  3. If no archive can meet the first and second criteria, system chooses archive quality higher than the first criteria, but the closet one to play.

Starting a Recording

You can start recording in HARMAN Media Suite using one of the methods:

- Call from HARMAN Media Suite to an interoperable endpoint from the Admin Portal.
- Call from HARMAN Media Suite to an interoperable endpoint from the User Portal.
- Call HARMAN Media Suite from an interoperable endpoint.
- Start a recording from the Collaboration Server (RMX) system using the recording link.
- Schedule a meeting on HARMAN Media Manager and connect the HARMAN Media Suite to an endpoint.

Start a Recording from the Admin Portal

You can start a recording from the admin portal.

Procedure

1. Access HARMAN Media Suite Admin Portal by its IP address or host domain name from a compatible browser.
2. Enter the user name and password to log in to the system.
3. Go to **Home.** In the **Signaling Connection** area, click **Dial out to record**.
4. Configure the dial out settings, as shown next:

Dial Out Parameters

Parameter	Description
Address	Specify the calling address. The system supports entering the calling address with an extended service number in the address box. If you call an H.323 system, you can dial out to endpoints by entering the numbers in the following formats: • [far end E.164 prefix] - Use when every system has registered to a gatekeeper. For example, if a far end system E.164 prefix is 9988. • [Far End H.323 ID]- Use when every system has registered to a gatekeeper. For example, if a far end system H.323 ID is CS9988. • [Far End IP Address]- Use when a system has not been registered to a gatekeeper. For example, if a far end system IP address is 172.22.33.44.
Signal	Set the H.323 or SIP network type for the system to place a call. Your choice depends on the call type used by the peer device.
VRR Name	Select a virtual recording room (VRR). You can use the built-in default VRR, or one you have created. A VRR defines recording policies. For more information, refer to Working with Virtual Recording Rooms (VRRs).
Distribution Template	Select a distribution template for the system to place a call.
Max Call Rate (Kbps)	Display the maximum call rate specified in VRR.

5. Click **OK**.

Start recording from an Endpoint

You can start recording by dialing HARMAN Media Suite or dial in to a VRR directly to start recording.

Procedure

- Enter the E.164 prefix or H.323 ID or SIP URL of HARMAN Media Suite on the user interface of an interoperable endpoint, for example, from remote control of HDX or Group Series.

  If your system or endpoint is not registered to the gatekeeper or to a SIP server, call the system IP address instead.

You can also dial in to a VRR directly to start recording by dialing one of the following:

For H.323 calls:

- `[HARMAN Media Suite IP]##[VRR number]`

  For example, if the `HARMAN Media Suite IP is 11.12.13.14`, and if the VRR number is `4096`, dial *`11.12.13.14##4096`*.

- `[HARMAN Media Suite E.164 prefix][VRR number]`

  For example, if the HARMAN Media Suite E.164 prefix number is 8888, and the VRR number is 4096, dial *`88884096`*.

For SIP calls:

- `[VRR number]@[HARMAN Media Suite IP]`

  For example, if the `HARMAN Media Suite IP is 11.12.13.14`, and the VRR number is `4096`, dial *`4096@11.12.13.14`*.

- `[SIP peer prefix][VRR number]`

  If the system has been registered to a SIP server, the SIP server should configure HARMAN Media Suite as a SIP peer. For example, if the SIP peer prefix of the HARMAN Media Suite system is 8888 and the VRR number is 4096, the dial string should be 88884096.

Peer-to-Peer Recording

Peer-to-peer recording allows a user to dial out to two endpoints from the HARMAN Media Suite Admin Portal or User Portal, and record the two sites into same recording file.

For now peer-to-peer recording is available only in H.323 peer-to-peer calls. For peer-to-peer recording from the user portal, refer to the HARMAN Media Suite User Guide.

Procedure

1. In the address line, enter the system's IP address in this format: https://<system IP address or FQDN>/admin.
2. Enter the user name and password to log in to the system.
3. Go to **Home or Call.** In the **Signaling Connection** area, click **Start Peer-to-Peer Recording**.
4. Enter the addresses of the two H.323 endpoint participants.
5. Click **OK**.

Live Streaming

Topics:

The HARMAN Media Suite system supports live streaming of video sources, such as live video conference or dual stream sent by endpoints, or MCUs with a highest resolution of 1080p and a maximum bandwidth of 4M.

These live streaming videos are saved in the system.

Configure Live Streaming

Before start live streaming from User Portal, follow the procedures below to configure the live streaming

Working with Recording Template

You can configure recording template to enable live streaming when recording.

Configure Live Streams in the Recording Template

You can configure a recording template-enabled live streaming and get live streaming by starting a call using the recording template.

Procedure

1. Go to **Template > Recording Templates**.
2. Select a recording template.
3. Click **Edit**. Select **Enable Live Streaming**.
4. Go to **Live Streaming (MP4)** and select **Enable H.264 High Profile for Live Streaming**.
5. Set **Primary Streaming Rate** and **Secondary Streaming Rate.**
6. In standalone mode, go to **Live Streaming (WMV)** and configure relevant settings.
7. Click **OK**.

Configure Audio-only Live Streams in the Recording Template

You can configure an audio-only live stream using a recoding template.

Procedure

1. Go to **Template > Recording Templates**.
2. Select a recording template.
3. Click **Edit**. Select **Enable Live Streaming**.
4. Select **Audio Only** in the **Call** tab.
5. Click **OK**.

Working with Distribution Template

The HARMAN Media Suite provides Flexible Stream Routing Policy, and distribution template defines the sites, which can get the live streaming and player policy for playing live in the routing policy.

Distribution template provides the following functions:

- Applying your live topology policy to Media Node eCDN sites.
- Configuring policy rule explicitly for players if a policy other than default rule is required for players in certain site.
- Defining multicast through site for one live event.
- Checking the LIVE topology once LIVE is ongoing.

Configure a Distribution Template

You can configure distribution templates.

Procedure

1. Go to **Template > Distribution Templates**.
2. Click **Add**.
3. Specify a unique name in **Template Name** to identify this template.
4. Select the **Live Topology** tab.
   a. Select a site to which you want to distribute streaming and click **Add** or double click the site to add the site in the template. If the child site is selected, the parent site is added automatically.
   b. Select the Multicast TTL value for the site.
      - If **Off** is selected, the system disables the Multicast (default setting).
      - If **On-Auto-Use System Setting** is selected, system uses the multicast configuration in **Configuration > Multicast Settings**.

      The routers must be configured correctly before enabling the multicast option for the site.
   c. Configure live streaming server and CDN (publish point).
      - Click **Add** in the **Live Streaming Server** tab to add Wowza as the live streaming server. The publish point can be a static publish point or a dynamic publish point, and you can get the value from Wowza.

- Click **Add** in **CDN** tab to add Akamai, CloudFront, or Edgecast as a CDN server and create a stream alias (local name for the stream). The publish point is a static publish point, so this template could be used by one concurrent live streaming only; any extra one will be rejected.

  Only available in a non-default distribution template.

If a static publish point is configured in the distribution template, the template is the static template, and only one live streaming event is allowed to use this template. If configured as a dynamic publishing point, then multiple live streaming could be setup through this template.

5 Select the **Player Policy** tab to configure the live streaming player policy. Player policy determines where the player in a certain location receives a stream. It is separate from the stream topology built-up. A player who is in a site that does not have a streaming server available could still be providing the stream by policy.

a Click **Add** to add a new policy.

b Select a site from drop-down list. The policy takes effect for the players located in the site.

c Select **Primary Policy** and **Fallback Policy**.

When the player in one site tries to play the live streaming, the system will first return the streaming URL followed by the Primary Policy. If the player cannot play the live streaming, then the system will return the streaming URL followed by the Fallback Policy.

The default policy is: Primary Policy is E-CDN only, and Fallback Policy is Global. If any site requires a policy different from the default policy, configure it here.

Player Policy for one Site

Primary Policy	Fallback Policy	Implementation
E-CDN only	Global	Streaming servers in the site load balance the streaming service first; if the whole site load reaches the threshold, a random selected streaming server URLs with the live streaming is sent to the player.
	3rd External Server Only	If the site capacity load reaches the threshold, a third external server provides the streaming service to the new coming player in the site.
	CDN Only	If the site capacity load reaches the threshold, the CDN server provides the streaming service to the new coming player in the site.
	Block	If the site capacity load reaches the threshold, a new coming player cannot play the live.

Player Policy for one Site

Primary Policy	Fallback Policy	Implementation
3rd External Server Only	Global	A third external server provides the streaming service to the player in the site first; if the site capacity load reaches the threshold, a random selected streaming server URLs with the live streaming will be sent to the player.
	CDN Only	A third external server provides the streaming service to the player in the site first; if the site capacity load reaches the threshold, CDN provides the streaming service to the player in the site.
	Block	A third external server provides the streaming service to the player in the site first; if the site capacity load reaches the threshold, new coming player cannot play the live.
CDN Only	-	Only the CDN provides the streaming service to the player in the site.
Block	-	The player in the site cannot play the live event.

   d Click **OK** to save the player policy.

6 Click **OK** to save the new distribution template.

Edit a Distribution Template

You can edit a distribution template.

Procedure

1. Go to **Template > Distribution Templates.**
2. Select the distribution template you want to change.
3. Click **Edit** or **Delete**.

Delete a Distribution Template

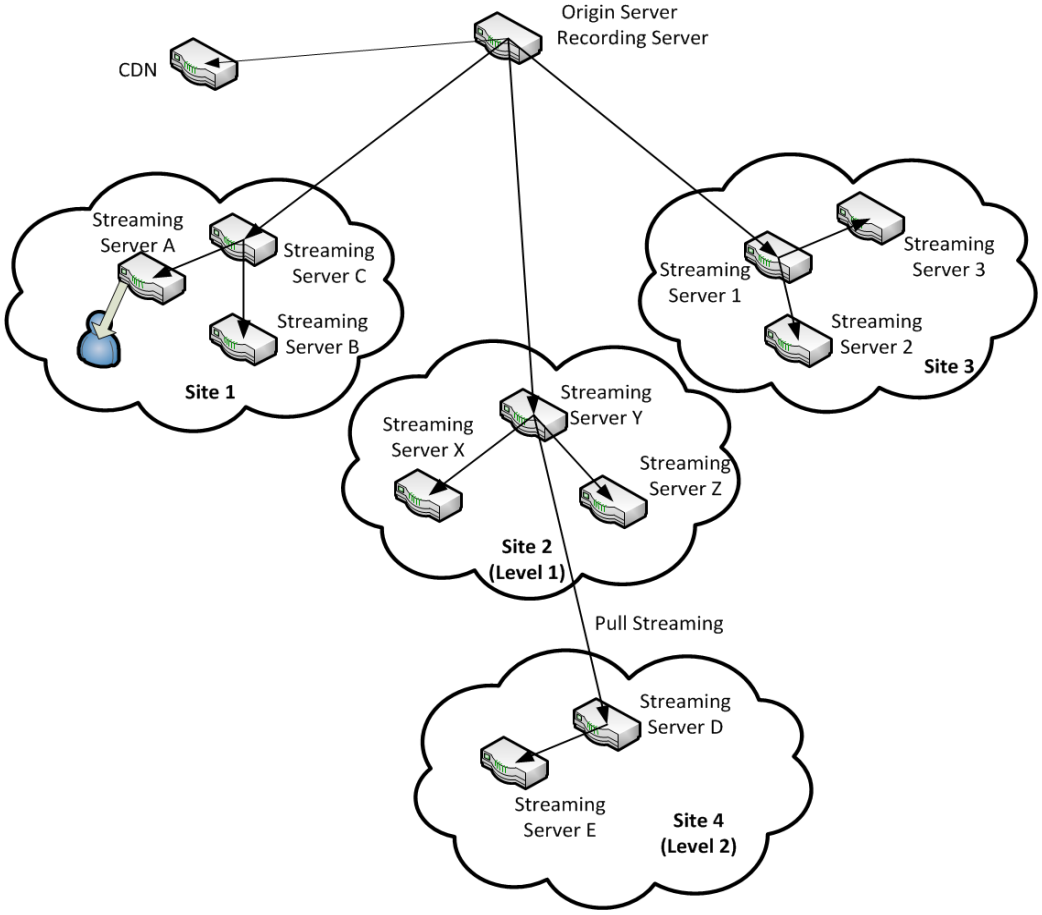
You can delete a distribution template.

Procedure

1. Go to **Template** > **Distribution Templates**.
2. Select the distribution template you want to delete.
3. Click **Delete**.

Working with eCDN

The enterprise Content Distribution Network (eCDN) is enabled in Scalability Mode. By distributing streaming to different sites, eCDN enables high capacity of concurrent streaming sessions (up to 50,000) for a single live event, and a user can get live streaming from nearest location. The eCDN also can support distributing a VOD file to different Media Nodes in site. Therefore, users can get VOD steaming from the nearest location. The following figure shows a typical network topology example of eCDN.



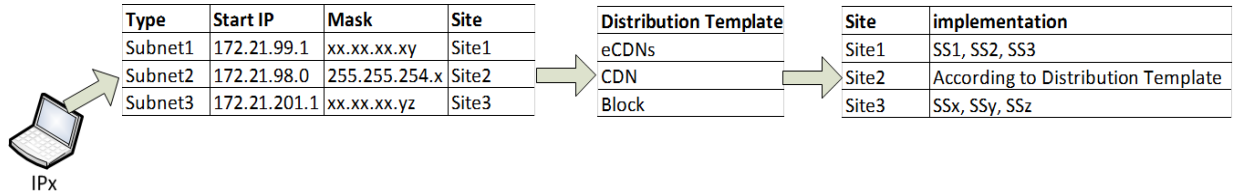
In previous example, the origin streaming server is the physical server that works as the recording server of the call. Site 1, Site 2, Site 3 and Site 4 are configured in distribute template as candidate sites. Site 4 is the child site of Site 2, which is configured in **Site Topology**.

The eCDN works as follows:

1. At the time the call is setup, according to the configuration in distribute template, Streaming Server C, Streaming Server Y, and Streaming Server 1 are selected as the proxy server of Site 1, Site 2, and Site 3 per policy (for example, load balance), and proxy servers will pull stream from origin server.
2. Proxy server in the site pushes stream to other streaming servers.
3. Streaming Server D is the proxy server in Site 4, and pull streaming from Streaming Server Y which is the proxy server in the parent site.
4. End-users who request the stream are directed to streaming server in the site.

The following shows an example about how to redirect an end-user to streaming server per location:

Redirect an End-user to Streaming Server



- Client (with IPx) accesses the streaming URL from HARMAN Media Suite User Portal.
- HARMAN Media Suite maps the IPx to subnet 2, and gets the Site 2 information through mapping table. Therefore, the player is in the site2.

  The mapping table between subnet and site could be imported from an excel file (CSV), or input manually through **Site Topology** > **Sites**.

  The mapping table between streaming server and site could be manually input by admin, or automatically matched by searching the streaming server IP address in the subnet list, and mapping it to the related entry. The unmatched streaming server falls into default site.
- HARMAN Media Suite Center checks the site 2 player policy configured in Distribute Template, and provide the streaming service according to the settings.

Player Policy for one Site

Primary Policy	Fallback Policy	Implementation
E-CDN only	Global	Streaming servers in the site load balance the streaming service first; if the whole site load reaches the threshold, a random selected streaming server URLs with the live streaming will be sent to the player.
	3rd External Server Only	If the site capacity load reaches the threshold, third external server provides the streaming service to the new coming player in the site.
	CDN Only	If the site capacity load reaches the threshold, CDN server provides the streaming service to the new coming player in the site.
	Block	If the site capacity load reaches the threshold, new coming player cannot play the live.

Player Policy for one Site

Primary Policy	Fallback Policy	Implementation
3rd External Server Only	Global	Third external server provides the streaming service to the player in the site first, If the site capacity load reaches the threshold, a random selected streaming server URLs with the live streaming will be sent to the player.
	CDN Only	Third external server provides the streaming service to the player in the site first, If the site capacity load reaches the threshold, CDN provides the streaming service to the player in the site.
	Block	Third external server provides the streaming service to the player in the site first, If the site capacity load reaches the threshold, new coming player cannot play the live.
CDN Only	-	Only CDN provides the streaming service to the player in the site.
Block	-	The player in the site cannot play the live.

Distribute Live Stream to eCDN

In eCDN topology, after starts a live stream, the sites get the streaming according to the configuration in the Distribution Template, so that the user can view the live faster, since the player could get stream locally and avoid delay.

Configure Live and Player Policy in Distribution Template

You can configure live and player policy in Distribution Template.

Procedure

1. Go to **Template** > **Distribution Template**.
2. Select a distribution template and click **Edit**.
3. Choose sites from **Site Policy** list, and click **Add** to add sites.

   After the sites are selected, the live streaming using the VRR will be pushed to these sites. The HARMAN Media Suite Center will choose one streaming server according to the idle capacity in the site as repeater.

Start Live Streaming with eCDN

You can start live streaming with eCDN.

After the live streaming or recording is done, you can play it from the user portal. The player will follow the Distribute Template configure to get live streaming

Procedure

1. Start a live streaming or recording with the VRR configured sites from User Portal or Admin Portal.
2. From the **Media > Live Streaming**, click **Detail** of one live streaming to view the repeaters involved in this live streaming, and its site information.

   When start a live streaming or a recording, the HARMAN Media Suite Center will select a Media Node as the recording server in the same site as the far-end at first.

   Note: HARMAN Media Suite treats Easy Capture live streaming in eCDN differently

   If a live event is created by Easy Capture, HARMAN Media Suite will select the closest streaming server based on the easy capture client location as the original streaming server. Users in other sites, will use streaming servers in own site to play streaming.

   If all streaming server resources in own site have been run out or there is no streaming server in own site, the play live streaming request will be rejected.

Distribute VoD to Sites

In eCDN topology, after the call is ended, the archive is hosted on the recording server. The archive could be replicated to other Media Nodes to accelerate the VoD access for potential remote users to play it. The replication process are by transcoding process including configuring the transcoding template, adding remote servers to the template, and attaching the template to VRR or doing dynamic archiving on Admin Portal.

Add Replication Server of VoD File in Transcoding Template

You can add a replication server of VoD file in a transcoding template.

Procedure

1. Go to **Template** > **Transcoding Templates**.
2. Create or edit a transcoding template, in **Transfer to Media Server** tab, select the servers to transfer archive.

   One media server (HARMAN Media Suite Center or media node) can support up to 1,000 concurrent streaming sessions, so if you expect more than 1,000 concurrent playbacks to same VoD file you can distribute the VoD file to other media server.

3. Click **OK** to save.

Add Transcoding Template in VRR

You can add a transcoding template in VRR.

Procedure

1. Go to **Template** > **VRRs**.
2. In **Transcoding Template** panel, select the created transcoding template.
3. Click **OK** to save.

Integrate eCDN with External Servers

HARMAN Media Suite can integrate with external media servers and public CDNs.

HARMAN Media Suite treats external media server (Wowza) and CDN (Akamai, CloudFront, and EdgeCast) differently:

- CDN can be used for global access, and can provide visiting out of enterprise network.
- External media server is treated as internal visit the same as HARMAN Media Suite streaming server.

Integrate eCDN with External Media Server (Wowza)

You can integrate eCDN with external media server (Wowza).

Make sure the external media server (Wowza) is set up correctly according to Configuring External Media Servers.

Procedure

1. If the subnets of the site have already covered the IP address of the Media Node, do not to add the subnet again, and go to Step 5. If not follow the step 2 to step 4 to add the subnet of the external media server (Wowza) as a streaming server.
2. (Optional) Go to **Site Topology** > **Sites**.
3. (Optional) Click **Add** to create a new site for external media server.
4. (Optional) Click **Add** under **Subnet** to add the subnet of the external media server (Wowza).
5. Configure external media server in distribution template to support playing live streaming.
   a. Go to **Template** > **Distribution Template**.
   b. Click **Add** in **Live Streaming Server** tab to add Wowza as live streaming server. The publish point can be static publish point or dynamic publish point, and you can get the value from Wowza.
   c. Make a call with this distribution template.

      If one static publish point is configured in the distribution template, the template is the static template, and can be used for only one live event.
6. Select external media server in the **Transfer to Media Server** tab.

   When the external media server is selected in transcoding template, the archive will be transferred to the external media server after transcoding is completed.
7. Play live streaming and VoD on the HARMAN Media Suite User Portal.

   The player policy for playing the live streaming follows the player configuration in distribution template.

Integrate eCDN with external CDN

You can integrate eCDN with external CDN.

Procedure

1. Make sure the CDN servers are set up correctly.

2. Go to **Template** > **Recording Templates**, and enable Live Streaming in the recording template.
3. Go to **Template** > **VRRs**, create a VRR and select the recording template.
4. Go to **Template** > **Distribution Templates**, and click **Add** in **CDN** tab to add Akamai, CloudFront, or Edgecast as CDN server, and create a stream alias (local name for the stream).

   The publish point is static publish point. Only available in non-default distribution template.

   If one static publish point is configured in the distribution template, the template is the static template, and can be used for only one live event.
5. Click **OK** to save.
6. Start a recording dialing out from User Portal using the distribution template with CDN configured.
7. Play the live streaming on HARMAN Media Suite.

The player policy for playing the live streaming follows the player configuration in distribution template.

Configure VRR

Configure a VRR with distribution template, and start a live streaming with the VRR from User Portal.

Live Stream Meetings to an External Server

Live streaming supports dual streaming rates which allows you to choose the appropriate bandwidth to view video according on your network condition.

Procedure

1. Configure the external media server on the HARMAN Media Suite system and enable live streaming.
2. Configure a recording template that enables live streaming.
3. Configure a distribution template that enables the external media server.
4. Record a meeting using the VRR that has the external media server enabled.

   Configure the external media servers to work with the HARMAN Media Suite system, as described below.

Start Live Streaming

Live streaming can only be started from User Portal.

For more information, see the *HARMAN Media Suite User Guide*.

View Live Streaming Information

If live streaming is in progress on the system, the current live streaming list displays on the live streaming page.

From **Media > Live Streaming** go the live streaming page.

The live streaming list displays the live streaming summary, such as live streaming name, VRR number used, start time, live streaming detail, and distribution template.

Working with Multicast

The HARMAN Media Suite system supports the multicast function and can perform the one-to-many transmission of video streams.

The system needs to send the video streams only once so that multiple computers can simultaneously share live streaming, which greatly reduces the demand for transmitting network video streams and saves the network bandwidth.

Before Using the Multicast Function

Meet the following requirements to use the multicast function successfully:

- The multicast function is activated in the HARMAN Media Suite system. Contact your supplier to obtain this function.
- Routers and switches in the network of client computers are configured to support the IP multicast communication with the HARMAN Media Suite system.

Configure the Multicast

Before you use the system to perform the multicast, configure the settings on the multicast page. Multicast can be configured in a site which has a HARMAN streaming server deployed. The system multicast setting below is a default setting that can be used with **Auto** option in each site policy in distribution template.

Procedure

1. Go to **Configuration > Multicast Settings**.
2. Configure the multicast settings:

Multicast Settings

Parameter	Description
Multicast IP Pool Starting Address	Specify the initial IP address of the multicast address pool. The system uses consecutive addresses starting with this IP address to perform the multicast. The maximum system supported multicast is the same as the maximum system supported live streaming. The starting IP address impacts the supported multicast number, for example, if the multicast address starts from 239.255.255.255, there is only one multicast is supported. One live streaming corresponds one multicast. The valid starting IP address range is 233.0.0.0 - 239.255.255.255.
Multicast TTL.	Specify the TTL value: • **Local Network -- 1** • **Intranet -- 32** • **Internet, Inter-continent -- 64** • **Internet, Inter-continent -- 128** • **Maximum allowed value -- 255 (default value)**

Note: Cannot start or stop the multicast manually

You cannot start or stop the multicasts manually, because they will start once the live streaming starts and will stop after the live streaming stops.

Multicast of a Live Streaming

The HARMAN Media Suite system supports the video multicast function and can send video streams to a group of computers at the same time.

Users can start a multicast from the live streaming list. The maximum system supported multicast is the same as the maximum system supported live streaming. Streaming format is defined in recording templates.

Note: Cannot support VoD archive multicast

VoD archive multicast is not supported.

Start a Multicast

You can start a multicast simultaneously while live streaming with a VRR.

Procedure

1. Create a distribution template with **Enable Multicast** selected.
2. Configure **Multicast TTL** from distribution template. Select **Auto** means using the system setting above.
3. Create a VRR with the configured recording template and distribution template.
4. Start live streaming with the VRR, and multicast starts at the same time.

Viewing a Multicast Streaming

If the site which HARMAN Media Suite Player is located enables the multicast in distribution template, the player can play the multicast streaming directly.

The HARMAN Media Suite Player on PC can receive MP4 multicast stream. If other players are used, the unicast stream will be given to the player. Using HARMAN Media Suite Player can save bandwidth by receiving multicast.

If there are MP4 and WMV streams in standalone mode, there will be two multicasts for the two stream types. If there are two bitrate streams, center chooses the higher bitrate stream on which to multicast. Currently, Media Player on Chrome/Firefox/Edge supports multicast streaming on Windows 10 by installing the Harman Multicast Plugin from player. The version of Edge should be (88.0.705.56 or later) which is based on Chromium.

Media Management

Topics:

You can archive your conferences and manage your archives.

Manage Archives

You can view all files recorded by the HARMAN Media Suite system on the **Media > Archives** page.

An administrator can delete or transcode these media files.

View Archive Details

1 Go to the **Media > Archives** page, administrators can view a summary of each archive by click , shown here.

Archive Details

Parameter	Description
ID	The ID for this archive.
Name	The name of the archive.
Duration	The duration of the archive.
Video Type	The video codec type used by the archive.
Audio Type	The audio codec type used by the archive.
Content Type	The content video type of the archive.
Key Words	The keywords for this archive.
Description	Additional user information.

Delete Archive Files

You can delete archives recorded by your own VRR, or archives that you are authorized to modify.

Procedure

1. Go to **Media > Archives**.
2. Select the archive files you want to delete.
3. Click **Delete**.

   The Confirmation page which list all deleted files pops up for second confirmation.
4. Click **OK** at the prompt message.

   The archive will be deleted permanently if be deleted from Admin Portal.

Transcode the Archive

You can transcode the archive files.

Procedure

1. Go to **Media > Archives**.
2. Select one archive file you want to transcode.
3. Click **Transcode**. All available videos with different formats are shown in the pop-up page.
4. Select one archive which you want to transcode, and click **Add**.
5. Select one or several templates that you want to use for transcoding, and click **Add** to start the transcode procedure.
6. Click **Close** to close the transcoding window.

Transcoding Task Control

In this section you can learn how to view transcoding status, stop an ongoing transcoding, or restart a transcoding.

View Transcoding Status

You can view the transcoding status of media file.

You have to wait for a long time if too many transcoding tasks are waiting in the queue.

Procedure

1. Go to **Media > Transcoding.**
2. In the archives list, select an archive.
3. Click **Media Files**. Media files transcoding can have the following status:
   - Ready: File can be played and downloaded.
   - Waiting: File waiting to be transcoded.

- Transcoding: File in transcoding.
- Error: File with transcoding error.
- Stopped: File creation stopped.

4 Click **Close** to exit the **Media Files** window.

Stop an Ongoing Transcoding

You can stop an ongoing transcoding process of media file which already in the Transcoding process or is in Waiting status.

Note: Cannot stop transcoding files
You cannot stop transcoding files of the status **Error** or **Stopped.**

Procedure

1 Go to **Media > Transcoding**.
2 Click a media file of the status **Transcoding** or **Waiting**, and then click **Stop-transcode**.
3 Click **OK,** and then click **Close**.

Restart Transcoding

You can restart the transcoding process for a media file.

Note: Cannot restart transcoding
You cannot restart transcoding for files of the status **Transcoding** or **Waiting**

Procedure

1 Go to **Media > Transcoding**.
2 Click a media file to be restarted, and then click **Re-transcode**.
3 Click **OK,** and then click **Close**.

Backing Up and Restore Media Files

The HARMAN Media Suite system is able to back up media data and system configuration to the FTP server in the network, and restore system user data, system configuration, and channel and category mapping relationship to the selected snapshot (based on the time points generated in the backup). HARMAN Media Suite uses only passive mode FTP to transfer files.

Configuring an FTP Server for Backup

Before backing up user data, you need to first configure FTP server on the HARMAN Media Suite system first.

The HARMAN Media Suite system supports the following FTP servers:

- 3CDaemon
- FileZilla Server
- Serv-U
- vsftpd

Backing Up and Restore Archives

There are three ways to back up archives on the HARMAN Media Suite system to an FTP server:

- **Automatic Archive:** Automatic backup the archive after the transcoding tasks are done, and delete the archive from HARMAN Media Suite.
- **Automatic Media Backup:** This is an incremental backup. Users can specify a **Frequency** of less than 7 days, and start time is available in one-hour increments.
- **Manual Media Backup:** Back up archives file manually. Includes full backup and incremental backup, and it applies to both NFS and RAID storage.

Back Up Archives Automatically After Call (Automatic Archive)

You can automatically back up the archive files after the call.

Once this function is enabled, archives will be transferred to the configured FTP server and removed from local disk after call, which is done automatically.

Procedure

1. Go to **Admin > Data Backup/Restore**.
2. From the drop-down list, select **Automatic Archive**.
3. Configure the following settings for the primary both FTP server and the alternate FTP server.

FTP Server Parameters

Parameter	Description
Server Address	Enter the IP address of the FTP server.
Port	Enter the port of the FTP server.
Media Backup Path	Specify the default FTP directory to save your media files.
User Name	Enter the account and password for login to the FTP server. **Note:** The registered FTP user should possess read-write permissions to the user root directory.
Password	
Use Anonymous	When this is enabled, you can log in to the FTP server using an anonymous account.
Test	Test whether the FTP configurations is functional.

4. Finish **Alternate FTP Server Configuration** if needed.
5. Click **Update**.

Once this function is enabled, archives will be transferred to the configured FTP server and removed from local disk after call, which is done automatically.

Back up media files automatically (Automatic Media Backup)

You can automatically back up media files.

Procedure

1. Go to **Admin > Data Backup/Restore**.
2. From the **Backup Type** drop-down list, select **Automatic Media Backup**.
3. Configure the following settings:

Parameter	Description
Server Address	Enter the IP address of the FTP server.
Port	Enter the port of the FTP server.
Media Backup Path	Specify the default FTP directory to save your media files.
Use Anonymous	When this is enabled, you can log in to the FTP server using an anonymous account.
User Name	Enter the account and password for login to the FTP server. **Note:** The registered FTP user should possess read-write permissions to the user root directory.
Password	
Test	Test whether the FTP configurations functions.
Frequency	Select how often the automatic media backup should be done, starting from 1 hour to a maximum of 7 days.
Start Time	Select the start time of automatic backup.

4. Click **Update**.

   The system restarts to apply your changes.

Back up the Archives Manually (Manual Media Backup)

You can manually back up archived media files.

If there are no archive in the system, backup will fail.

Procedure

1. Go to **Admin > Data Backup/Restore**.
2. From the **Backup Type** drop-down list, select **Manual Media Backup**.

3 Configure the following settings:

FTP Server Parameters

Parameter	Description
Server Address	Enter the IP address of the FTP server.
Port	Enter the port of the FTP server.
Media Backup Path	Specify the default FTP directory to save your media files.
Use Anonymous	When this is enabled, you can log in to the FTP server using an anonymous account.
User Name	Enter the account and password for login to the FTP server. **Note:** The registered FTP user should possess read-write permissions to the user root directory.
Password	
Test	Test whether the FTP configurations functions.

4 Click **Full backup** or **Increment backup**.

You can see the backup status in **Backup/Restore Status**. The system archives file are backed up to the configured FTP server.

If no archive in the system, backup will fail.

Restore the Archives

You can restore the backed up archive files.

Procedure

1 Go to **Admin > Data Backup/Restore > Restore**.

2 Choose a restore point from the drop-down list.

3 In Scalability Mode, select one device or all from **Restore Sub-point by Device** to restore media data.

4 Click **Restore**.

If you restore archives from the version earlier than version 2.8, the mapping relationship between archives and category cannot be restored.

System Administration

Topics:

System Version Management

You can use this feature to switch to different HARMAN Media Suite versions.

If you want to migrate the system from HARMAN Virtual Edition/Docker Edition to the HARMAN Media Suite EVO, contact your HARMAN Sales Representative or Authorized HARMAN Reseller to implement the operation. (This function is not ready on Media Suite EVO 4.2.1)

Before you switch your system version, you should always back up your settings and recordings.

HARMAN is not responsible for any user data loss during these operations.

Switch system version by upgrade package

Procedure

1. Go to **Admin > System Version Management**.
2. View the HARMAN unified EULA info and agree to it.
3. Click **Open** and select the software upgrade package mediasuite-x.x.x-version.tar.gz file to upload.
4. Once the uploading is done, Click **Update Version** to confirm the action.
   The system performs the upgrade and reboot automatically. This may take several minutes.
5. Enter your administrator **User ID** and **Password** and then click **Log In**.
6. To confirm that the system is upgraded, check the software version on the **Product Activation** page.

For scalability mode, both the HARMAN Media Suite Center and the media node software must be the same at all times. If the HARMAN Media Suite Center gets upgraded or downgraded, the media node must also get upgraded or downgraded.

Upload Plugin

Administrator can upload HARMAN Media Suite Player plugin or Easy Capture Application for user download.

After plugin is uploaded, user can download the plugin from user portal.

Procedure

1. Go to **Admin > Plugin/Application Upgrade**.
2. Click **+ Add**, and select a plugin.zip file from the pop-up window.
3. Click upload to upload plugin to User Portal. After plugin is uploaded, user can download the plugin from User Portal.

Restart the System

You can restart your system.

Procedure

1. Go to **Admin** > **Restart/ShutDown**.
2. Read the risk of restart and click **Restart Media Suite**.
3. Click **OK** at the prompt message.

Shut Down the System

You can shut down the system.

Before unplugging the HARMAN Media Suite, you need to shut down the server in the admin portal. If the HARMAN Media Suite does not restart after reboot or an upgrade, unplug the HARMAN Media Suite, wait for about five minutes, plug in the HARMAN Media Suite, and then reboot.

Procedure

1. Go to **Admin** > **Restart/ShutDown**.
2. Read the risk of shutdown and click **Shutdown Media Suite**.
3. Click **OK** at the prompt message.
4. You can restart or shutdown a specific server by reboot the device.

Maintenance of the System

The HARMAN Media Suite provides a way to maintain the system, you can set the restart time and recurrence pattern.

HARMAN Digital Transformation Solutions

Procedure

1. Go to **Admin > Maintenance**.
2. To schedule the maintenance, select the **Maintenance** check box.
3. Choose restart time in your time zone.
4. Choose recurrence pattern.
5. Click **Update**. The maintenance will take place as per the schedule.

Backing up and Restore System Configuration

You can back up and save the system configuration of HARMAN Media Suite system to your local computer so that you can restore the configuration if necessary. Supported configurations include:

- Hard disk warning threshold
- IP setting parameters
- System time
- Recording settings
- Certificate, port and security policy
- Gatekeeper, SIP, and QoS settings
- Site topology and device manager configuration

The Enterprise Directory users who are granted permission cannot be backed up when you back up the system configuration. You have to back up Grant Permission AD users manually before backing up system configuration.

Back Up the Current System Configuration

You can back up the current system configuration.

Procedure

1. Go to **Admin > Configure Backup/Restore**.

   The configuration file will be stored on the local machine that the browser is running on.
2. Click **Backup**.

   System backs up the configuration file along with the media files when dose Automatic Media Backup or Manual Media Backup. If system crash unexpected, administrator can get the recovery copy from the FTP server.

Disable backup file type

You can select the type of files that are not to be backed up, the four types are RAW, M4A, MP4, WMV.

Procedure

1. Go to **Admin > Configure Backup/Restore**

2 Select files you do not want to back up.
3 Click **Back up**, the selected types for file will not be backed up.

Restore System Configuration

You can restore the system configuration of the HARMAN Media Suite.

The system only can restore the configuration of current version, but cannot restore from the configuration file of previous version.

Procedure

1 Copy the configuration file (.ppm file) from **Config** folder in FTP server to your local PC.

HARMAN recommends to use the configuration file which is backed up along with media files on the backup FTP server, **so you can easily restore the media files matched with configuration**.

2 Log in to the Admin Portal.
3 Go to **Admin > Config Backup/Restore**.
4 Click **Add**, select the .ppm file from local machine and click **Open**.
5 Click **Upload**.
6 Click **Restore.**
7 Confirm to restart the system.

System and Archives Recovery for Device Replacement

HARMAN Media Suite provides several methods to recover your data and system configuration.

If HARMAN Media Suite (HARMAN Media Suite Center or Media Node) is damaged unexpected, and have to be replaced with a new server, you can follow the procedures to recover your system:

- You can only restore the configuration file which is backed up from other server once, that is, if you replace the HARMAN Media Suite server, you cannot restore the configuration file backed up from other server to the new server the second time.
- You can only restore the configuration to the same HARMAN Media Suite version only.
- For HARMAN Media Suite Center Replacement, the Local Users could not be available by this method. If you still need that information, you need to record them down, delete them and then re-create. HARMAN will try to support it in a future release.

Procedure

1 Install hardware and software, and active the license for the new server.
2 Restore configuration file.
3 Active the system license from **Admin** > **Product Activation**.

Restart the system.

4. For HARMAN Media Suite Center Replacement) Reset Portal Admin Password, Refer to Reset Portal Admin Password on page 161.
5. Check IP and Media Storage configuration.
   a. Go to **Device** > **Device Manager**.
   b. Select the device and click **Edit**.
   c. Make sure the **Network Settings** and **Media Storage** configuration is your desired configuration, or update the configuration.
6. (For HARMAN Media Suite Center Replacement) Recall Media Nodes.
   a. Go to **Device > Device Manager**.
   b. Select all Media Nodes.
   c. Select **Action > Recall** to register all Media Nodes to new HARMAN Media Suite Center. It will take several minutes for all Media Nodes register correctly.
7. Restore archives.
   a. Go to **Admin > Data Backup/Restore > Backup**.
   b. Update FTP information.
   c. Click **Restore** tab.
   d. Select the restore point. The time should be the same as the configuration file which you just restored.
   e. Select **All** from **Restore Sub-point by Device**.
   f. Click **Restore**.

      System restores your media files.

HARMAN Digital Transformation Solutions

Monitoring the System

Topics:

Check Real-time System Status on the Home Page

You can find real-time system status and information on the Home Page of the Admin Portal.

Signaling Connection

The signal connection provides information and the recording status of the calls to and from video endpoints or MCUs with this HARMAN Media Suite.

Procedure

1 Click to expand detailed information.

Signal Connection Parameters

Parameter	Description
Far End Number	The far end number used by the connection
Start Time	The time the call started
Signaling Type	H.323 or SIP
Dial In/Out	Whether the connection is incoming or outgoing
VRR Number	The VRR number used by the connection
Live Streaming	Whether the connection is performing live streaming
Detail	Additional information like VRR name, audio type, audio call rate, video type, video call rate, etc
Real Time Information	Displays the call address, audio packet loss, video resolution, video frame rate, etc

2 Control the recording using the buttons shown next:

- Start recording
- Pause recording

- Resume recording
- Stop recording
- End the connection

3 Dial out to connect the endpoint to record using **Dial out to record**.

4 Control the Quick Code playback using the buttons shown next:

- Pause playback
- Resume playback
- Stop playback
- Start playback
- Fast backward playback
- Fast forward playback
- End the connection

You can control the Collaboration Server (RMX®) playback using the buttons shown next:

- Pause playback
- Resume playback
- Stop playback
- Fast backward playback
- Fast forward playback
- Change conference layout
- End the connection

System Information

You can view the basic system information.

Displays the following basic system information:

- System name
- The current version of the software running on the system
- The maximum number of recording ports and live streaming ports supported by the system
- Licensed recording ports and live streaming ports usage

System Alerts

Shows the system alert summary and detailed information, for example, registration to primary gate-keeper failed, LAN2 failed to acquire DNS automatically, IP address conflict for LAN1, CPU usage is too high, memory usage is too high, NFS connection is lost, temperature is out of range, log size has reached the threshold value.

Please see information below about some of the common alerts, their possible causes and suggested resolutions.

System Alerts

Alert	Possible Causes	Suggested Resolution(s)
Registration to primary gate-keeper failed	• Gatekeeper Server is unreachable. • Gatekeeper port is blocked (By firewall or changed in Gatekeeper server, default value is 1719) • Gatekeeper rejects MS's registration request	• Ping to Gatekeeper address from Media Suite to check the connection. Check with IT team why it's unreachable • Catch network trace for register action and analyze the pcap file • Set a alternate gatekeeper, then if the primary gatekeeper has some issues, it will switch to the alternate gatekeeper.
NTP server is unreachable	• NTP server is unreachable • NTP port is blocked (123 port) • If NTP address is set as FQDN, DNS might be not available or set incorrectly	• Ping to NTP address from Media Suite to check the connection. Check with IT team why it's unreachable. • Catch network trace for set NTP server action and analyze the pcap file • Set correct DNS to parse NTP FQDN
vDisk mount lost	Mounting local disk failed	Please check and remount local disk manually by following steps: **1. Run df command to check whether the /var/localmedia folder is mounted to device /dev/sdb** -bash-4.1# df Filesystem 1K-blocks Used Available Use% Mounted on none 8129936 1496 8128440 1% /dev/shm /dev/sda3 10320640 7135160 3185480 70% /data /dev/sda3 10320640 7135160 3185480 70% / tmpfs 8129936 1496 8128440 1% /dev/shm /dev/sda2 1032064 107576 924488 11% /config /dev/sda5 10320640 296788 10023852 3% /database /dev/sda6 41280000 5966908 35313092 15% /output tmpfs 8129936 1496 8128440 1% /dev /dev/sda2 1032064 107576 924488 11% /etc/polycom-msc /dev/sda2 1032064 107576 924488 11% /usr/polycom-msc/res /dev/sda6 41280000 5966908 35313092 15% /var/log /dev/sda6 41280000 5966908 35313092 15% /var/tmp /dev/sda6 41280000 5966908 35313092 15% /var/mail-box /dev/sda6 41280000 5966908 35313092 15% /var/userdata /dev/sda6 41280000 5966908 35313092 15% /var/install /dev/sda7 19571744 197372 19374372 2% /dump /dev/sda7 19571744 197372 19374372 2% /var/log/tcpdump /dev/sda7 19571744 197372 19374372 2% /var/nginx /dev/sda3 10320640 7135160 3185480 70% /var/media /dev/sdb 41153856 9236296 29804024 24% /var/localmedia

Alert	Possible Causes	Suggested Resolution(s)
		2. If there is no localmedia disk mounted, Run lsblk command to check if there is device sdb -bash-4.1# lsblk NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT sda 8:0 0 120G 0 disk |-sda1 8:1 0 32M 0 part |-sda2 8:2 0 1G 0 part /config |-sda3 8:3 0 10G 0 part /data |-sda4 8:4 0 1K 0 part |-sda5 8:5 0 10G 0 part /database |-sda6 8:6 0 40G 0 part /output `-sda7 8:7 0 19G 0 part /dump sdb 8:16 0 40G 0 disk /var/localmedia sdc 8:32 0 5G 0 disk sr0 11:0 1 1.3G 0 rom loop1 7:1 0 1.3G 0 loop 3. If there is sdb disk, Run following command to remount the local media disk mount -t ext4 /dev/sdb /var/localmedia 4. Then check if there are contents in the local media folder ls -l /var/localmedia 5. If there are media files and folders listed in above step, then reboot Media Suite. Finally check whether the warnings are removed.

Alert	Possible Causes	Suggested Resolution(s)
Log size has reached the set threshold value	Used log file space is larger than 21 GB	Remove some unused log files by **Auditor** account.
The hardware capacity of the recording port does not meet license capacity requirements.	• The hardware's CPU and Memory could not meet the requirement of higher license, for example, a 8 Core/16 GB Media Suite virtual machine cannot have 18/9 license. • Some nodes are down/offline and then we could not have enough node to support the license. • Service on some nodes is not available and then we could not have enough services to support certain license. • If the LTI Support license item is enabled in Product Activation page, it requires to regenerate the license key without LTI Support. (4.2.1 version)	• Increase the CPU and Memory capacity. • Check if all the nodes are one from Device Manager page, and might need to reboot some of them. • Check if recording service in some nodes is down; check if the disk is mounted and reboot the service • Contact HARMAN Support to regenerate the license key if LTI Support is enabled in the Product Activation page (4.2.1 version)

Signaling Server Status

Displays gatekeeper registration status and SIP server registration status. When the H.323 registration is successful, the system’s E.164 prefix and H.323 alias are displayed.

Hardware Status

Checks the hardware status using the following indicators:

- **Basic**
  - **CPU Usage**
  - **Memory Usage**
  - **System Disk Usage**

- **Extension:** Specifies value, disk, local media disk, power.

Web Connections

Displays connection status on the Admin Portal for administrators and auditors.

- Admin Portal Connections:
  - Current Administrators
  - Current Auditors

External Server Status

The system can be integrated with external servers. You can check the configuration for WOWZA, AKAMAI, EdgeCast, Active Directory (AD) server, and CloudFront, respectively.

Configure SNMP

Your system provides a standard Simple Network Management Protocol (SNMP) interface which supports SNMP version 1, version 2, and version 3 queries with confidentiality, authentication, and integrity functions conforming to SNMP MIB.

The interface uses a common MIB, making it interoperable with CMA, DMA, and Collaboration Server (RMX) systems. Available configurable options vary with the SNMP agent version and security level selected.

Configure SNMP Agent Settings

You can configure SNMP agent settings.

Procedure

1. Click **Configuration > SNMP**.
2. Select **Enable SNMP**.

   SNMP is disabled by default.
3. Configure the SNMP **Agent** settings:

SNMP Agent Settings

Parameter	Description
Retrieve MIB Files	Retrieve MIB file to your computer.
Agent Name	Specify the name of this HARMAN Media Suite agent.
Device Location	Specify the location for this HARMAN Media Suite.
Contact Person	Specify a contact person for this HARMAN Media Suite.
SNMP Agent Version	Specify the SNMP Agent version.
Accepted Host Community Name	Specify the community name that the host belongs to.

Parameter	Description
User Name	Specify the user name that will be used to log in over the **Authentication Protocol**.
Authentication Protocol	Specify the type of encryption to use when connecting with this user: • **MD5**: Message Digest 5 • **SHA**: Secure Hash Algorithm
Authentication Password	Specify the password that will be used to log in over the **Authentication Protocol**. **Note**: A valid password contains 8-64 characters, and does not include these characters: &,',",<,>,%,|,+,=
Privacy Protocol	Specify the privacy protocol that you want to use: • **DES**: Data Encryption Standard • **AES**: Advanced Encryption Standard
Privacy Password	Specify the password that will be used to log in over the privacy protocol. **Note**: A valid password contains 8-64 characters, and does not include these characters: &,',",<,>,%,|,+,=

Configure SNMP Trap settings

You can configure SNMP trap settings

Procedure

1. Click **Configuration > SNMP**.
2. Select **Enable SNMP**.

   SNMP is disabled by default.
3. Configure the following SNMP trap settings, as shown next:

SNMP Trap Settings

Parameter	Description
Address	Enter the IP address of the SNMP server.
Port	Specify the port for SNMP trap.
SNMP Agent Version	Specify the SNMP Agent version.
Community Name	Specify the community name which is the same in SNMP server.
User Name	Specify the user name that will be used to log in over the **Authentication Protocol**.
Transport Protocol	Specify the transport protocol.
Authentication Protocol	Specify the type of encryption to use when connecting with this user: • **MD5**: Message Digest 5 • **SHA**: Secure Hash Algorithm

SNMP Trap Settings

Parameter	Description
Authentication Password	Specify the password that will be used to log in over the **Authentication Protocol**. **Note**: A valid password contains 8-64 characters, and does not include these characters: &,',",<,>,%,|,+,=
Privacy Protocol	Specify the privacy protocol that you want to use: • **DES**: Data Encryption Standard • **AES**: Advanced Encryption Standard
Privacy Password	Specify the password that will be used to log in over the privacy protocol. **Note**: A valid password contains 8-64 characters, and does not include these characters: &,',",<,>,%,|,+,=

Besides standard SNMP MIB files, HARMAN Media Suite also provides two proprietary MIB files:

- HARMAN-BASE-MIB.mib
- HARMAN-REAL-PRESENCE-MONITORING-MIB.mib

To use these HARMAN MIB files, first import the file HARMAN-BASE-MIB.mib, then HARMAN-REAL-PRESENCE-MONITORING-MIB.mib. Otherwise, the HARMAN MIB files cannot be correctly compiled.

All HARMAN Media Suite MIB files can be downloaded from the Admin Interface under **Configuration > SNMP > Retrieve MIB Files**.

Troubleshooting

Topics:

System Log Configuration

The logger utility is activated at the system startup and continually records system events.

The log files generated by the utility contain the following information:

- Events occurred in system internal modules.
- Administrator activities.
- System login attempts.
- Operation errors.

All log files generated the day prior are automatically compressed into a ZIP file named year-month-date.tar.gz at log maintenance window every day. The log maintenance window is usually the first hour from 00:00:00 system time every day.

The log file storage is 30GB. You are prompted when the system reaches the storage limit. The system will delete the old logs to free the disk space at log maintenance window.

Configure Log Settings

You can change the system logging strategy, configure warning limit, and also enable remote login.

Procedure

1. Go to **Admin** > **Log Settings**.
2. Configure the following settings:
   - Logging Level: Specify the system logging level, which decides to what level system events should be written into the center/server.log file.
     - **Info** - logs all non-debug messages.
     - **Debug** - logs all messages.
     - **Error** - logs the fewest number of messages.
     - **Warning** - logs between error and Info messages.

- Logger Warning Capacity: Specify the percentage of log file capacity used at which the system displays a warning on the dashboard.
- Log retention period (days): Defines the number of days to keep log archives on server.
- SysLog Server IP Configuration: To configure the IP settings of the SysLog server.

Log Management

The following table shows actions that administrators and auditors can perform.

Log Management

Action	Description
Refresh	Refreshes the list and adds newly generated log files.
Download	Downloads the selected log file.
Download Today's Logs	Downloads all the log files generated today.
Delete	Delete selected system logs. Only audit can delete the system log.

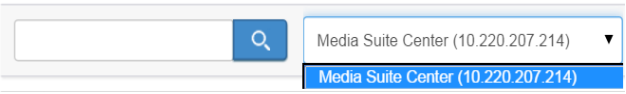
Download Log Files

You can download the log files.

Procedure

1. Go to **Admin > System Logs**.
2. In scalability mode, select the server you want to gather the logs from.

   System Logs

3. In the **Log** list, select the log to be saved.
4. Click **Download**, or click **Download Today's Logs** to download all that day's logs.

Note: From the version 3.4.3, download behavior changes as described below and it impacts on config file and mib file download in the Admin Portal.

- On starting a download, a new tab/window (depending upon the browser preferences) is opened to inform user about the download status.
- The download-status messages are localized based on the language selected by the user on the portal language preferences.
- The tab/window will be automatically closed after the download is completed.
- The user may close the tab/window in between while the download is in progress, the ongoing download will not be impacted. If the tab/window is manually closed, the download will still continue in the background.
- To abort or cancel the download in between, the user can close or refresh (F5) the main tab/window from which the download was initiated.
- Once the download is completed, the file will be available in the browser's download tray for Save, Open or Cancel option, or Auto-saved and Open option (depending on browser's preferences).
- In case an error occurs while downloading, the tab/window will automatically close after showing a brief failure message, and no file will be available in the browser's download tray or an unnamed raw-file available in the browser's download tray.
- For troubleshooting download-failures, users are requested to contact the Harman MediaSuite Support Team (to debug browser console logs).

Delete Log Files

You can delete the log files.

Procedure

1. Log in as audit.
2. Select one or several log files.
3. Click **Delete** to delete the selected log files.
4. Click **OK** on the pop-up confirmation page to delete the log files.

   System cannot delete the log file being used.

System Log Backup

The HARMAN Media Suite system is able to back up the system logs zip of daily logs package.

Procedure

1. Go to **Admin > System Logs Backup > Backup**
2. Configure the following settings:

- **Server Address**: Enter the IP address of the FTP server.
- **Port**: Enter the port of the FTP server.
- **Media Backup Path**: Specify the default FTP directory to save your media files. For multiple nodes, the system creates respective folders for those nodes to save respective system log packages.
- **Use Anonymous**: When this is enabled, you can log in to the FTP server using an anonymous account.

- **User Name/Password**: Enter the account and password for login to the FTP server.

  Note: The registered FTP user should possess read/write permissions to the user's root directory.
- **Test**: Test whether the FTP configurations function
- **Frequency**: Select the period for automatic backup in days
- **Start Time**: Select the start time of automatic backup

3 Click the **Update** button.

The system auto backups the system log zips into the ftp server according to the config info.

System Diagnostics

HARMAN Media Suite provides ping, traceroute command, and network traffic capture to troubleshoot network issues, and to gather diagnostics information for further troubleshooting.

Execute Ping or Traceroute on the Device

You can execute the ping or traceroute commands on the device to troubleshoot network issues.

Procedure

1 Go to **Admin > Diagnostics.**

2 Select the **Device Name** from which pings are sent.

3 Enter the IP address or host name you want to ping.

4 Select **Ping** or **Traceroute**.

5 Click **Start** to execute the command. The result is shown in the **Result** area.

Execute a network traffic capture

You can execute a network traffic capture to troubleshoot network issues.

Procedure

1 Go to **Admin > Diagnostics.**

2 Select **Network Traffic Capture**.

3 Select the **Device Name** from which the network traffic capture is sent.

   Select **All** means that the Network Traffic Capture is executed simultaneously if additional Media Nodes are attached to the HARMAN Media Suite Center.

4 Enter the **Capture Duration (Minutes)**.

   The max is 30 minutes.

5 Enter the filter that is used sent to the .pcap00 file, and the file can be viewed by Wireshark.

The filter depends on the Linux command *tcpdump*. You can use every filter which is used by tcpdump. More information about tcpdump, refer to http://linux.about.com/library/cmd/blcmdl8_tcpdump.htm.

Note:
The network traffic capture function should not be used when there are more than 5 recordings ongoing in parallel.

Rebuild RAID for the HARMAN Media Suite Appliance Edition

HARMAN Media Suite Appliance Edition supports RAID 10 (RAID1 for the 6/3 port license, which is available in the specific market).

This section explains when you should rebuild RAID, how to replace failed hard disks, and how to rebuild RAID.

- Rebuild RAID Conditions
- Replace a Hard Disk
- Rebuild RAID

Rebuild RAID Conditions

Two TB hard disks are used as one RAID logical unit. It supports up to four TB of storage (two for the 6/3 port license, which is available in the specific market) TB storage. Each hard disk is marked with a number as shown in the following illustration.

Hard Disk Number for RAID 1

Hard Disk Number for RAID 10

You can see the status of each hard disk on the Admin Portal. See Hardware Status for details. If the status of a hard disk is “error”, you need to remove this hard disk and order a new one.

Note: Shut down before change hard disks

- Shut down your HARMAN Media Suite before you change hard disks. HARMAN Media Suite does not support hot swapping.
- Contact your local HARMAN representative to order a replacement hard disk.

After you use new hard disks, the system may need to rebuild RAID and data may be lost, as shown in the following table.

Rebuild RAID 1

User Case	Rebuild RAID?	Lost Data?	Does HARMAN Media Suite go back to work immediately?
Replace one hard disk.	No	No	Yes After you replace the hard disk and reboot the system, the system needs to reorganize the data on the new hard disk. The RAID status is Degraded (Recovering).
Replace two hard disks when RAID fails.	Yes	Yes	Yes After you replace the hard disks and reboot the system, the system will go to the recovery mode. You need to rebuild RAID under the recovery mode manually, which takes 10 minutes. After rebuilding RAID, the system will go back to work. You lost all the previous data. The status of RAID is Normal (Resyncing). It takes about 4 to 5 hours to finish the resyncing process.

Rebuild RAID 10

User Case	Rebuild RAID?	Lost Data?	Does HARMAN Media Suite go back to work immediately?
Replace one hard disk.	No	No	Yes After you replace the hard disk and reboot the system, the system only needs to reorganize the data on the new hard disk. The RAID status is Degraded (Recovering).
Replace two hard disks when RAID is degraded.	No	No	Yes After you replace the hard disks, HARMAN Media Suite will send an email to remind you restart the system. After you reboot the system, the system only needs to reorganize the data on the new hard disk. The RAID status is Degraded (Recovering).

User Case	Rebuild RAID?	Lost Data?	Does HARMAN Media Suite go back to work immediately?
Replace two hard disks when RAID fails.	Yes	Yes	Yes After you replace the hard disks and reboot the system, the system will go to the recovery mode. You need to rebuild RAID under the recovery mode manually, which takes 10 minutes. After rebuilding RAID, the system will go back to work. You lost all the previous data. The status of RAID is Normal (Resyncing). It takes about 4 to 5 hours to finish the resyncing process.
Replace more than two hard disks.	Yes	Yes	Yes After you replace the hard disks and reboot the system, the system will go to the recovery mode. You need to rebuild RAID under the recovery mode manually, which takes 10 minutes. After rebuilding RAID, the system will go back to work. You lost all the previous data. The status of RAID is Normal (Resyncing). It takes about 4 to 5 hours to finish the resyncing process.

Replace a Hard Disk

If the status of a hard disk is “error”, you will see a hardware alert indicating failed hard disks after you log in to the Admin Portal. HARMAN recommends that you to replace all failed hard disks.

To replace a hard disk:

1. Shut down your HARMAN Media Suite.
2. Press the brown buckle on the front panel of HARMAN Media Suite as shown in Replace Hard Disk for RAID 1 illustration.

Replace Hard Disk for RAID 1

Replace Hard Disk for RAID 10

3 Pull out the hard disk.

4 Unscrew the three screws on both sides of the hard disk as shown next.

Unscrew Hard Disk

5 Replace the failed hard disk by screwing a new hard disk to the tray.

6 Insert the hard disk back to its slot.

Rebuild RAID

When one or more hard disks does not work, you will see a hardware alert indicating failed hard disks on the Admin Portal. You need to replace failed hard disks and reboot HARMAN Media Suite, the RAID status will change to Degraded or the system will go to the recovery mode in case of RAID failure. This always means that you need to rebuild RAID.

To rebuild RAID:

1 Replace failed hard disks.

2 Restart your HARMAN Media Suite.

3 Connect an empty USB key to the HARMAN Media Suite system and reboot to get to the recovery mode.

4 Enter your password to log in the recovery mode after the system is restarted. The default password is `SUPPORT`.

5 Check the RAID status under the recovery mode. Click **Hardware Diagnose** on the left, you will see the hardware status as shown in the following illustration. Only when the RAID status is `FAILED`, you need to rebuild RAID.

RAID Status

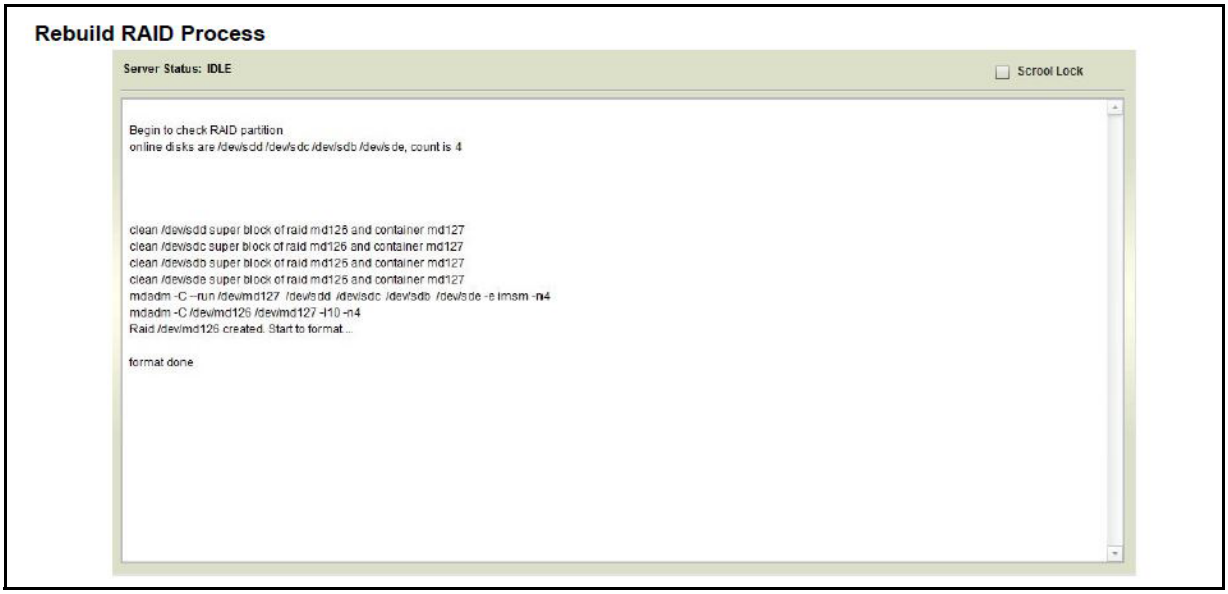
6 Select **Reset Raid Storage** on the left as shown next.

Rebuild RAID

7 Click **Yes** to rebuild RAID.

You will see all the detailed information in the **Server Status** panel. After the rebuilding RAID process done, you will see the message `format done` and the server status will returns to `IDLE` as show next.

Rebuild RAID Process



Click **Reboot System**. Your HARMAN Media Suite will go back to work.

Appendix A – Console Commands

Topics:

The HARMAN Media Suite supports essential system configuration by using Console.

You can access Console using VGA or SSH, some popular applications like Putty supports SSH.

Login Console

The login interface shows all of the software information and you'll be prompted to enter the login password.

The user name and initial password to access console are harman/harman. You must change the initial password when you log into the console first time.

Note: Factory default password
The factory default login password is harman (case sensitive).

Log in to the HARMAN Media Suite Appliance Edition Console Using VGA

Procedure

1. Connect a monitor and keyboard to the HARMAN Media Suite system.
2. Enter the user name and password (both are **harman** by default)
3. Type **Alt+F2** keys to go to the main command menu.

Log in to Console Using SSH

You can log in console through SSH.

Procedure

1. Open SSH client, enter **Host Name** and **Port** (the default SSH port is 22).

2 Enter the user name and password (both are **harman** by default). You must change the initial password when you log into the console first time.

If you have completed all the above configurations and launched Console successfully, press the **Enter** key. The login interface appears.

Console Command

You can use the following commands for system configuration.

Set Server Role

Select **Set Server Role** and type **Enter** to set role of the server.

Procedure

1 Select **Media Node** or HARMAN Media Suite Center, and press **OK** to set the role of HARMAN Media Suite.

2 Set the HARMAN Media Suite Center IP address for Media Node, and click **OK**.

3 Click **Yes** to save the changes on the pop-up page.

4 Click **Yes** to reboot all services on the pop-up confirm page. All the services reboot, and then log off.

Configure Network Settings

You can use console command to configure network setting.

1 Select **Network Setting** and type **Enter** to set network configurations (DHCP IP address and static IP address) for LAN 1 or LAN 2.

Only for HARMAN Media Suite Center
In Scalability Mode, Network Settings is only available for HARMAN Media Suite Center.

Configure Static IP Address for LAN1 and LAN2

You can use console command to configure LAN IP address.

Procedure

1 Choose a network interface, click **OK** or type **Enter**.

2 Select **Static Address Setup**, click **OK** or type **Enter**.

3 Configure network settings.

Parameter	Description
IP Address	IP address of the network port
Subnet Mask	Subnet mask of the network port
Default Gateway	Gateway address of the network port

4. Click **Save configuration** if you are fine with the settings or **Cancel** to return.
5. The system will show the prompt message *Yes to save the configuration?* Choose **Yes** to proceed or **No** to cancel.
6. At the pop-up message, click **Yes** if you want the system to restart to apply your changes.

Configure DHCP IP Address for LAN1 or LAN2

You can use console command to configure LAN DHCP IP address.

Procedure

1. Choose a network interface, click **OK** and type **Enter**.
2. Select **DHCP Address Setup**, click **OK** and type **Enter**.
3. Click **Set To DHCP**.
4. The system will show the prompt message *Yes to save the configuration?* Choose **Yes** to proceed or **No** to cancel.
5. Click **Yes** if you want the system to restart to apply your changes.

Note: System restarts after setting the connection feature
After you set the connection feature or IP address for the LAN interface, the system must be restarted in order for the new settings to take effect.

Configure the DNS Server

You can use console command to configure DNS server.

Procedure

1. Choose **DNS Server** and press **Enter**.
2. Enter DNS server address for the system to resolve domain names.

Configure the Disk Usage

You can use console command to configure disk usage.

Procedure

- Choose **Disk Usage** and type **Enter** to view the disk space usage of HARMAN Media Suite.

  The total, used, and free disk space are shown.

Reset Console Password

This is to reset the console password.

Procedure

- Choose Reset Console Password and press Enter, and follow the prompt message to set new password to access console.

the system will show the prompt message to set new password to access console.

Reset Portal Admin Password

You can use console command to reset portal admin password.

Procedure

- Choose **Reset Portal Admin Password** and press **Enter**, and follow the prompt message to set new password to access the admin portal.

Reset Config

This is to reset the following system configurations to the default value:

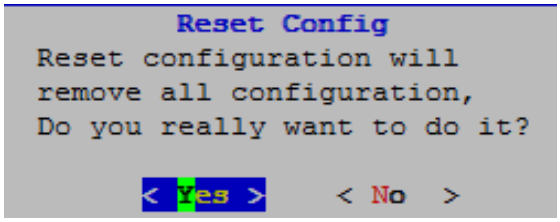
- System Config
  - Call Settings
  - Signaling Settings
  - Port Settings
  - System time
  - Media Storage Settings
  - Multicast Settings
  - Certificate Management
  - QoS
  - SNMP
  - Active Directory
  - Password Settings
  - Customization
  - Portal Settings
- Admin
  - Log Settings
  - License

- Template
  - Recording Templates
  - Transcoding Templates
  - Distribution Templates
  - VRRs
- Server
  - WOWZA
  - AKAMAI
  - EdgeCast
  - CloudFront
- User
  - User
  - Group

Procedure

1. Choose the item and press Enter to reset the configuration.

   The system will show the following prompt message:



2. Click **Yes** to proceed or **No** to cancel.

   After resetting the system configuration, the system must be restarted in order for the new settings to take effect.

Check the Network Connection Status

You can use console command to check the network connection status.

Procedure

- Choose **Ping** and type **Enter** to check the network connection status.

Reboot the System

You can use console command to restart the system.

Procedure

1. Choose **Reboot** and press **Enter** to restart the system.

   The system will show the prompt message *Do you really want to reboot the machine?*

2 Choose **Yes** to restart the system, or **No** to cancel.

Shutdown the System

You can use console command to shutdown the system.

Procedure

1 Choose **ShutDown** and type **Enter** to power off the system.
The system will show the prompt message *Do you really want to shutdown the machine?*
2 Choose **Yes** to restart the system, or **No** to cancel.

Restore the System to the Snapshot Creation Time

You can use console command to restore the system to the snapshot creation time.

Procedure

1 Choose **Fallback** and type **Enter** to restore the system to the time the snapshot was created.
2 Click **Yes** to fall back the system or **No** to cancel.

Restart All Processes

You can use console command to restart all processes.

Procedure

- Choose **Restart All Processes** and type **Enter** to restart all processes.

Stop all Processes

You can use console command to stop all processes.

Procedure

- Choose **Stop all Processes** and type **Enter** to restart all processes.

Show the General Information

You can use console command to show the general information.

Procedure

- Choose **Show** and type **Enter** to show the general system information including System Version, Interface Information, and IP Address Information.

Exit the Command Control Interface

You can use console command to exit the command control interface.

Procedure

- Choose **Exit** and type **Enter** to exit the command control interface.

Appendix B – Configure Wowza Media Server

Topics:

You can now stream live meetings and on demand meeting archives to leading third party media server Wowza. This feature expands the streaming audience capacity of the HARMAN Media Suite system.

Users can watch these streams and on demand meeting archives hosted on external media servers from within the Admin Portal, or from the User Portal.

For more information about HARMAN Media Suite and Media Manager integration, see the Integration Guide from HARMAN Support.

On the HARMAN Media Suite system, you can live stream recordings and push VoD recordings to the Wowza Media Server.

You can view the live streaming or archives from the User Portal of the HARMAN Media Suite system.

The section shows some useful examples to configure third party external media servers, for latest configuration details, refer to third party external media server documentations.

Note: External media servers are used after the HARMAN Media Suite reaches the capacity threshold

Live streaming uses HARMAN Media Suite resources first, after the resources reach the threshold, the external media servers are used and round robin among the external media servers.

Configure the Wowza Media Server

You need to configure the Wowza Media Server and your HARMAN Media Suite to work together.

Procedure

1. Install JDK and Wowza. Run

   `<Wowza directory>\examples\installall.bat` to create the needed configurations and directories.

Wowza Media Server Configurations and Directories

Parameter	Live Streaming	VoD
Application Name	live	VoD
Application Directory	<Wowza directory>\applications\live	<Wowza directory>\applications\vod
Configuration File Location	<Wowza directory>\conf\live\Application.xml	<Wowza directory>\conf\vod\Application.xml

2 To enable Wowza authentication, modify the configuration file as follows:

- For live streaming: Open `<Wowza directory>\conf\live\Application.xml`, set digest as the value for the tag `PublishMethod`. That is, `<PublishMethod>digest</PublishMethod>`.
- For VoD: Open `<Wowza directory>\conf\vod\Application.xml`, HARMAN recommends you not to set authentication, make sure `playmethod` is none, `<PlayMethod>none</PlayMethod>`
- Open `<Wowza directory>\conf\publish.password`, type the your user name and password.

3 To enable Wowza support with cross domain access, modify the configuration file as follows:

a Open the *application.xml* for live event and VoD, for example, the default application files for VoD and live event are `<Wowza directory>\conf\live\Application.xml` and `<Wowza directory>\conf\vod\Application.xml`. If you create other application files for VoD and live event, open the corresponding application.xml.

b Add the following properties to the **HTTPStreamer/Properties** container

```
<Properties>
<Property>
<Name>httpUserHTTPHeaders</Name>
<Value>Access-Control-Allow-Origin:*|Access-Control-Allow-Credentials:
true|Access-Control-Expose-Headers:Date|Access-Control-Allow-Methods:H
EAD, GET, POST|Access-Control-Allow-Headers:Overwrite, Destination,
Content-Type, Depth, User-Agent, X-File-Size, X-Requested-With,
If-Modified-Since, X-File-Name, Cache-Control, Range</Value>
<Type>String</Type>
</Property>
</Properties>
```

c Restart the Wowza Streaming Engine.

4 Install and configure a FTP server.

The FTP server shares the `<Wowza directory>\content` directory. You need to have at least the **Read, Write**, and **Create Directories authorities**.

The following example shows the configuration for a FileZilla FTP server.

5 Start the Wowza server.

When you see the message **Wowza media server is started!**, the server is configured successfully.

Enable Wowza support cross-domain access when playing live event or archive using Chrome.

Appendix C – Configure the Server Working with VCS

Topics:

This chapter demonstrates how to configure the HARMAN Media Suite working with Cisco TelePresence® Video Communication Server (Cisco VCS).

The configurations are different between H.323 and SIP.

Configure VCS for H.323 Calling

For H.323, after you register HARMAN Media Suite to the Cisco VCS, Cisco VCS works as a gatekeeper. you can configure the Cisco VCS and then call a VRR created on HARMAN Media Suite to start a recording.

Procedure

1. Create authentication accounts in VCS, such as ff1/1234, ff2/1234….ff6/1234.
2. Register HARMAN Media Suite to VCS.
3. Go to **Configuration > Signaling Settings** and set **Gatekeeper type** as **Cisco VCS.**
4. Register an endpoint to the VCS.

   For example, register HARMAN Group Series 500 to the VCS.

Now you can dial from the Group Series 500 and the format of the address is `E.164+VRR Number`. After the call is set up successfully, you can check the HARMAN Media Suite Admin Portal.

Configure VCS for SIP Calling

If your network supports SIP, you can use SIP to connect to conference calls. Cisco VCS works as a SIP server.

Procedure

1. Register HARMAN Media Suite to VCS via SIP.
2. Register an endpoint to the VCS via SIP. For example, register HDX 4000 to the VCS.
3. Configure the VCS to enable SIP calling.
   - **a** Log in to the Cisco VCS as an administrator.
   - **b** Go to **VCS Configuration > New zone** to create a new zone.

c Configure the zone for your HARMAN Media Suite. Refer to the following table.

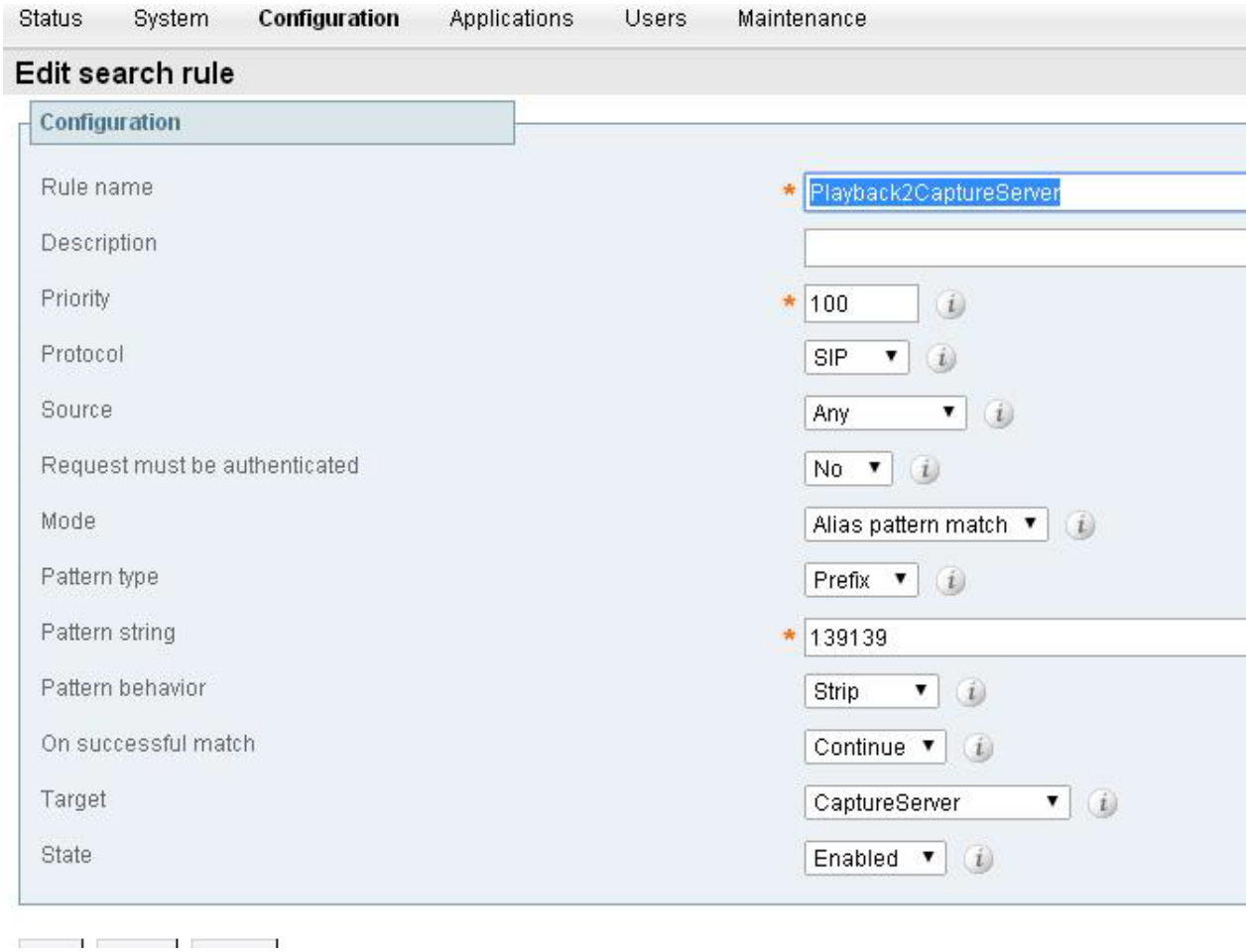
VCS Zone Parameters

Parameter		Settings
Name		media_suite_zone
Type		Neighbor
Hop count		15
H.323	Mode	On
	Port	1719
SIP	Mode	On
	Port	5060
	Transport	TCP
	Accept proxied registration	Allow
Authentication policy		Do not check credentials
SIP authentication trust mode		Off
Peer 1 address		Your HARMAN Media Suite IP address.
Zone profile		Custom

d Create a search rule to route to the zone you created.

The following example assumes that you have the default tandberg recommended rules in place.

Set search rule parameters



Now, you can start a recording by calling a VRR number from any endpoint registered to this Cisco VCS. For example, if the VRR number is 12345, you can dial `13913912345` directly to start a recording. 139139 is the prefix name (pattern string set in above picture).

Appendix D - Update Local Intranet Zone of Client for IWA

Topics:

Once you have set up the IWA configuration on the HARMAN Media Suite Admin Portal, you will need to update the Local Intranet zone on each client computer accessing the User Portal internally.

The Administrator also can login to each client computer joined to the domain, and use the following steps to update the settings.

Configure Internet Explorer of Each Client for IWA

You can configure the Internet Explorer browser for each client for IWA.

Procedure

1. In Internet Explorer, click **Tools**, and then click **Internet Options**.
2. Click the **Security** tab, click the **Local intranet** zone, and then click **Sites**.
3. Check **Include all sites that bypass the proxy server**.
4. Click **Advanced**.
5. In **Add this website to the zone**, enter the FQDN of the User Portal, such as *http://userportal.mediasuite.com*.
6. Click **Add**, click **Close**, and then click **OK**.
7. Click **Customer Level** in the **Security** tab.
8. Scroll down and select **Automatic logon only in Intranet zone** under **User Authentication**, and click OK.
9. Select the **Advanced** tab. Scroll down and verify that **Enable Integrated Windows Authentication** is checked.
10. Click **OK** to close the **Internet Options** dialog box.

The domain Administrator can use the following steps to use Group Policy to push IE browser setting to all internal client computers joined on the same domain.

Use the Group Policy to Update All Client Computers

You can use the Group Policy to update all client computers.

Procedure

1. Click **Start**, click **Administrative Tools**, and then click **Group Policy Management**.
2. Right-click the Group Policy Object (GPO) you use to publish changes to client computers in your domain and then click **Edit**.
3. Under **User Configuration**, expand **Policies**, expand **Windows Settings**, expand **Internet Explorer Maintenance**, and click **Security**, and then double-click **Security Zones and Content Ratings**.
4. Under **Security Zones and Privacy** select **Import the current security zones and privacy settings**.

   Read the information about enhanced security configuration carefully. If the local Intranet zone is considered a trusted zone without enhanced security configuration, click **Continue**. If the local Intranet zone requires enhanced security, follow the directions on this screen and click **Cancel**.
5. Click **OK**. Group Policy setting will refresh after 90 minutes. Clients can refresh immediately by running **gpudate** /**force**.

Configure Firefox for IWA

You can configure the settings for using IWA in Firefox browser.

Procedure

1. In Firefox, enter **about:config** in the address bar and accept the warning to enter the configure page.
2. Search *network.automatic-ntlm-auth.trusted-uris* in the search bar.
3. Double-click the preference name to open the **Enter string value** dialog.
4. Enter the FQDN of the User Portal, such as *http://userportal.mediasuite.com*.
5. Click **OK**.
6. Search `network.negotiate.auth.delegation-uris` and `network.negotiate-auth.trusted-uris`, and repeat steps 3, 4, and 5 to finish the configuration.

Configure Chrome on Mac for IWA

You can configure the settings for using IWA on Chrome browser in Mac systems.

Procedure

- Run command `defaults write com.google.Chrome AuthServerWhitelist -string '*.msdev.com'` on Mac.

Appendix E – Configure Lync Server for HARMAN Media Suite System

The HARMAN Media Suite can be deployed in Microsoft® Skype for Business and Lync environments.

This chapter shows you how to use Lync Server Management Shell commands to set routing for the HARMAN Media Suite system, which enables the HARMAN Media Suite system to receive Lync Server calls.

Configure the Lync PowerShell to Create the Trusted Application

You need to create the trusted application using the Lync PowerShell.

To create the trusted application:

1. Navigate to **Start > All Programs > Microsoft Lync Server 2013 > Lync Server Management Shell** to open the Lync PowerShell terminal.
2. Use the `New-CsTrustedApplicationPool` command to create a new pool that will contain the computers that host trusted applications.

   ```
   New-CsTrustedApplicationPool -Identity ms20696.sfb2015.com -Registrar
   Registrar:lync2015.sfb2015.com -site 1 -ComputerFqdn ms20696.sfb2015.com
   -ThrottleAsServer $true -TreatAsAuthenticated $true
   ```

   The parameters are defined as follows:

   -Identity The FQDN of the new pool. Enter the HARMAN Media Suite FQDN for the parameter. In this example, ms20696.sfb2015.com.

   -Registrar The service ID or FQDN of the Registrar service for the Lync server pool. In this example, lync2015.sfb2015.com.

   -Site The Site ID of the site on which this pool is homed.

   -ComputerFqdn Creating a trusted application pool will automatically create a trusted application computer that is part of that pool. By default, the computer will receive the same FQDN as the pool.

   -ThrottleAsServer Set this parameter to false to throttle connections between the servers within the pool and trusted applications as clients.

   -TreatAsAuthenticated Determines whether authentication is required for trusted applications connecting to servers within the pool.

   For more information about the `New-CsTrustedApplication` command, see Microsoft Lync New-CsTrustedApplicationPool.

3 Use the `New-CsTrustedApplication` command to set up a trusted application for the HARMAN Media Suite.

```
New-CsTrustedApplication -ApplicationId ms20696
-TrustedApplicationPoolFqdn ms20696.sfb2015.com -Port 5061
```

The parameters are defined as follows:

-ApplicationId A descriptive name for HARMAN Media Suite. Must be unique within your Lync deployment. In this example, ms20696.

-trustedApplicationPoolFQDN The FQDN of the application pool. Enter the HARMAN Media Suite FQDN for the parameter. In this example, ms20696.sfb2015.com.

-port The SIP port. The default SIP port number is 5061.

For more information about the `New-CsTrustedApplication` command, see Microsoft Lync New-CsTrustedApplication.

Configure Lync PowerShell to Update the Topology

You need to use Lync PowerShell to update the topology.

To update the topology:

1 Navigate to **Start > All Programs > Microsoft Lync Server2013 > Lync Server Management Shell** to open the Lync PowerShell terminal.

2 Use the `Enable-CsTopology` command to update the Lync topology.

```
Enable-CsTopology
```

Use Lync PowerShell to Define a Static Route for the HARMAN Media Suite

You need to define a static route for your HARMAN Media Suite solution using Lync PowerShell. Route changes you make take effect immediately.

To define a static route:

1 Navigate to **Start > All Programs > Microsoft Lync Server2013> Lync Server Management Shell** to open the Lync PowerShell terminal.

2 Use the `New-CsStaticRoute` command to set up a static route for the HARMAN Media Suite.

```
$route = New-CsStaticRoute -TLSRoute -destination "ms20696.sfb2015.com"
-port 5061 -matchuri "ms20696.sfb2015.com" -usedefaultcert $true
```

where the first `ms20696.sfb2015.com` is the FQDN of the HARMAN Media Suite server SIP signaling domain and the second `ms20696.sfb2015.com` is the name of the Trusted Application Pool you created.

For more information about the `New-CsStaticRoute` command, see Microsoft Lync New-CsStaticRoute.

3. Set the routing configuration. By configuring the static route, matched URI dialing is enabled.

   The following example sets the route to be global:

   ```
   Set-CsStaticRoutingConfiguration -identity global -route @{Add=$route}
   ```

4. To check that the commands were entered correctly in the PowerShell, enter: `Get-CsStaticRoutingConfiguration`.

   Static routes are not required for presence–enabled VMRs or for the HARMAN Media Suite-enabled conferences.

The HARMAN Media Suite solution is now set as a trusted host, and calls from a Lync client to a SIP address in the HARMAN Media Suite's domain will be routed through that system.

Appendix F– Third-Party Conference Recording Support

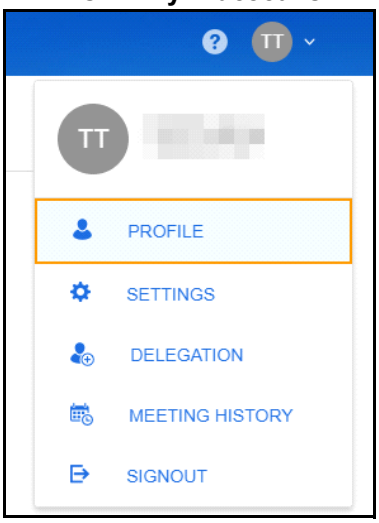
Third-Party Conference Recording Support - BlueJeans

Topics:

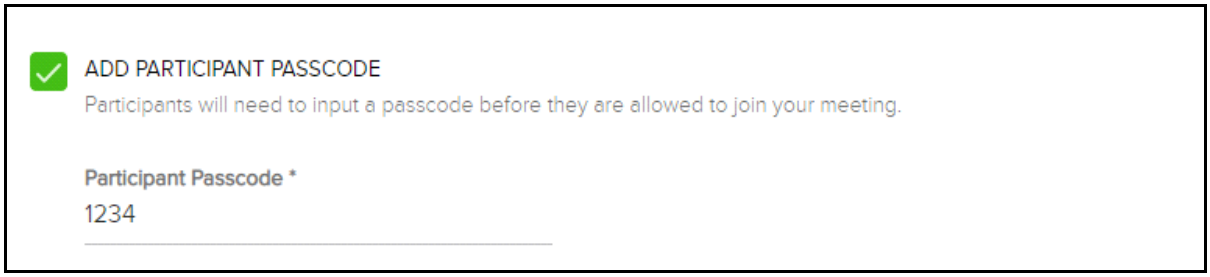
BlueJeans meeting settings

Before using the HARMAN Media Suite to record BlueJeans Meeting, we should know the following information related to your meeting room settings:

1. Go to BlueJeans website, https://www.bluejeans.com/ and login with your credentials.
2. Click **My BlueJeans** and select **SETTINGS**.



3. You can set **My Meeting ID, Participant Passcode** and other options if required.



Recording and Playback to BlueJeans meeting

BlueJeans supports signaling for SIP (TCP/ TLS) and H323, users can dial a record/live stream/playback calls to BlueJeans meeting on the HARMAN Media Suite User Portal. Before the call, follow the steps below:

- Go to the HARMAN Media Suite **Admin Portal > Configurations> Signaling Settings**, ensure that the SIP and H323 are not registered to any Gatekeeper or SIP server, the **Transport Type** for SIP is "TCP" or "TLS".
- Get the **Meeting ID** for your meeting, we can get the ID from BlueJeans desktop application or BlueJeans settings. (Refer to above topic: BlueJeans meeting settings)
- Ensure that your account has set the **Participant Passcode** for BlueJeans meeting. (Refer to: BlueJeans meeting settings)

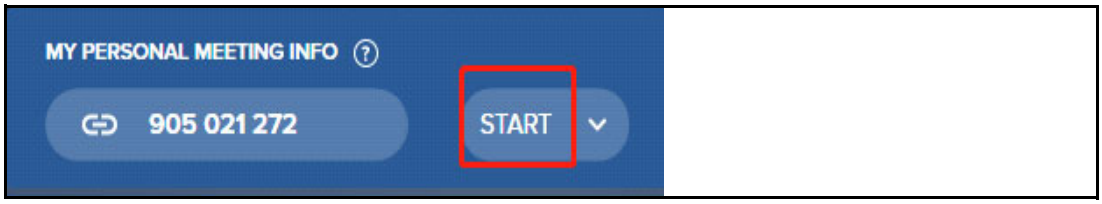
There are two methods to join and record BlueJeans Meeting

Join a meeting by Meeting ID (Recommended)

1 Start the BlueJeans meeting (two methods)

   a Go to BlueJeans website https://www.bluejeans.com/, login with your credentials. Click **START MY MEETING**

   b If BlueJeans desktop application already installed, open your BlueJeans desktop application **>** Click **START**



2 Dial from HARMAN Media Suite Side.

Media Suite Type	Connection Method	Example
Record/Live Playback to meeting	For SIP calls, if participant code is **NOT** set: <Meeting ID>@104.238.247.247 <Meeting ID>@bjn.vc	902021272@104.238.247.247 902021272@bjn.vnc
	For SIP, if participant code is set: <Meeting ID>.<Passcode>@<IP> <Meeting ID>.<Passcode>@bjn.vc	902021272.1234@104.238.247.247 902021272.1234@bjn.vnc
	For H323, if participant code is **NOT** set: IP##meeting ID	104.238.247.247##902021272
	For H323, if participant code is set: <IP>##<Meeting ID>#<Passcode>	104.238.247.247##902021272#1234

Join meeting with room style (Not recommended)

1 On your BlueJeans desktop application > Click **START**.

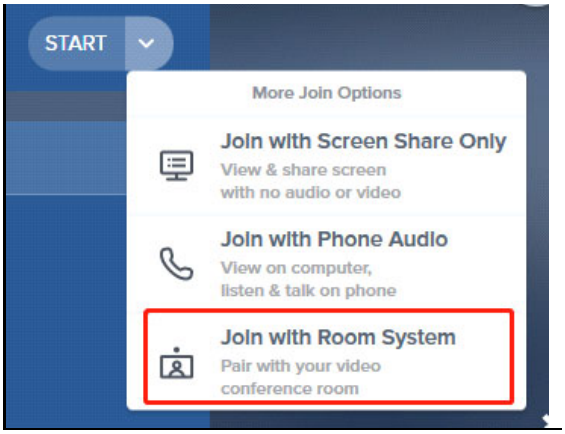
2 Dial from the HARMAN Media Suite:

Media Suite Type	Connection Method	Example
Record/Live Playback to meeting	For SIP calls, if participant code is **NOT** set: <Meeting ID>@104.238.247.247 <Meeting ID>@bjn.vc	902021272@104.238.247.247 902021272@bjn.vnc
	For H323, if participant code is set: <IP>##<Meeting ID>#<Passcode>	104.238.247.247##902021272#8111

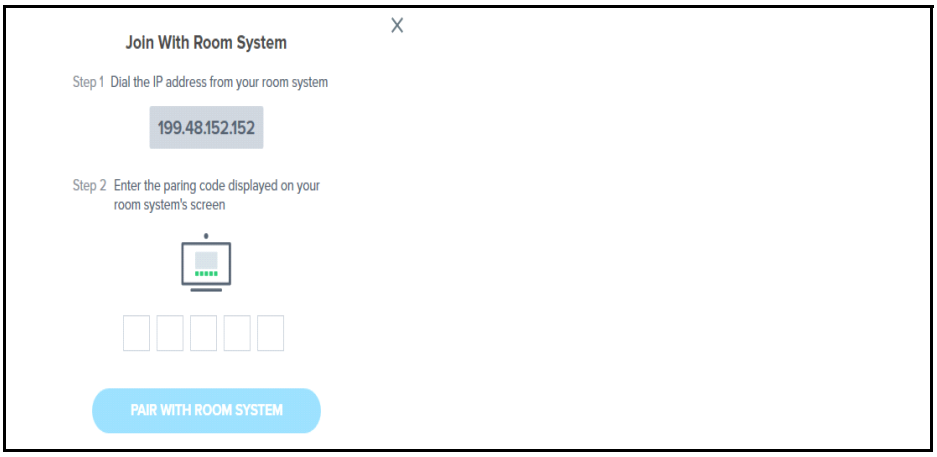
3 The HARMAN Media Suite enters the BlueJeans meeting lobby.

4 Login to the HARMAN Media Suite User Portal **>** Click your Avatar > **My Media Center > Events**, if you enabled the live streaming then we can preview the Live streaming and get 5 letters code from the live streaming video (such as: XESCC)

5 On the Bluejeans desktop application, join a meeting with room style mode.



6 Enter the 5 letter passcode to start the meeting.



Third-Party Conference Recording Support - GoToMeeting

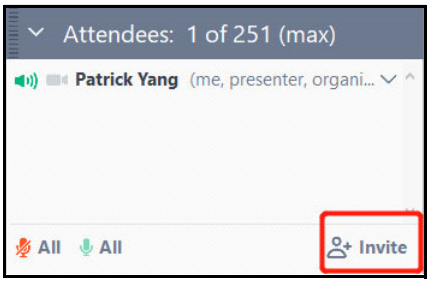
Topics:

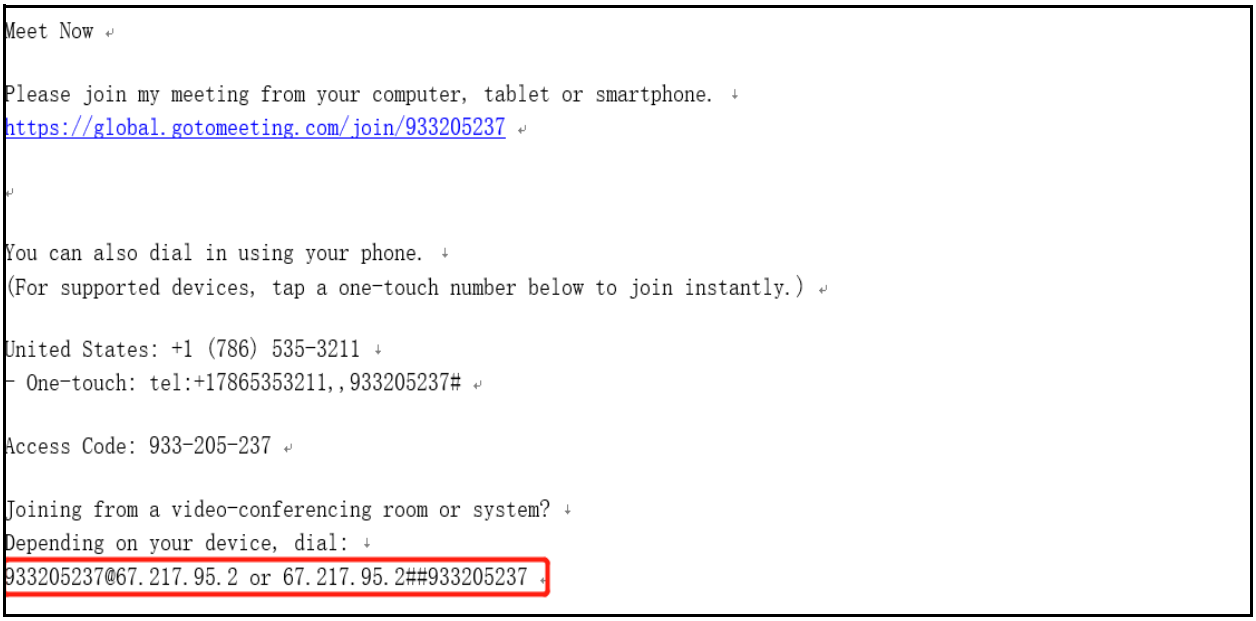
- Recording and Playback to GoToMeeting

Recording and Playback to GoToMeeting

The HARMAN Media Suite only support H323 calls to GoToMeeting conference.

1. Login to the GoToMeeting account on you GoToMeeting desktop application.
2. Click **meet now** to start the meeting,
3. Get the **meeting ID** and **GoToMeeting IP** by clicking the function icon "Invite+", click Email and check.





4 Dial from the HARMAN Media Suite side for record/live/playback

- <GoToMeeting IP>##<Meeting ID> (e.g.: 67.217.95.2##160644621)
- <Meeting ID>@<GoToMeeting IP> (e.g.: 160644621@67.217.95.2)

5 The call has been established.

Third-Party Conference Recording Support - Cisco Webex Meetings

Topics:

- HARMAN Media Suite Configuration for support Cisco Webex Meetings
- Recording and Playback to Webex Meetings

HARMAN Media Suite Configuration for support Cisco Webex Meetings

The HARMAN Media Suite only supports SIP (TCP/ TLS) calls to Webex Meetings. Before dial calls to Webex Meetings, confirm your configuration of signaling:

1. Go to the HARMAN Media Suite Admin Portal **> Configurations > Signaling Settings**, ensure that SIP and H323, are not registered to any Gatekeeper or SIP server, the **Transport Type** for SIP is "TCP" or "TLS".

Warning:

If no archive been recorded after the recording call or user can not watch anything on the live. Please consider setting the NAT address by below method:

2. Go to Admin Portal **> Device >** Select device and click **Edit**
3. Go to **Network Settings**, enable the option **NAT Public (WAN) Address** and fill the address, then **Save**
4. Go to **Configuration > Call Settings**, enable the option **NAT Enable**, then click **OK**

Recording and Playback to Webex Meetings

User can simply record/live/playback to Webex Meetings by dial below string format, just replace the **Meeting ID, Username, sitename** of your own.

- <Meeting ID>@[sitename].webex.com
- <Username>@[sitename].webex.com

Note:
If you face any issues in connecting to Webex meetings from HARMAN Media Suite, please try to change the **Preferred DNS Server** to 1.1.1.1 or 8.8.8.8 on the Admin Portal under **Device > Device Manager > Device Settings > Network Settings > General System Network Settings**.

Third-Party Conference Recording Support – Zoom

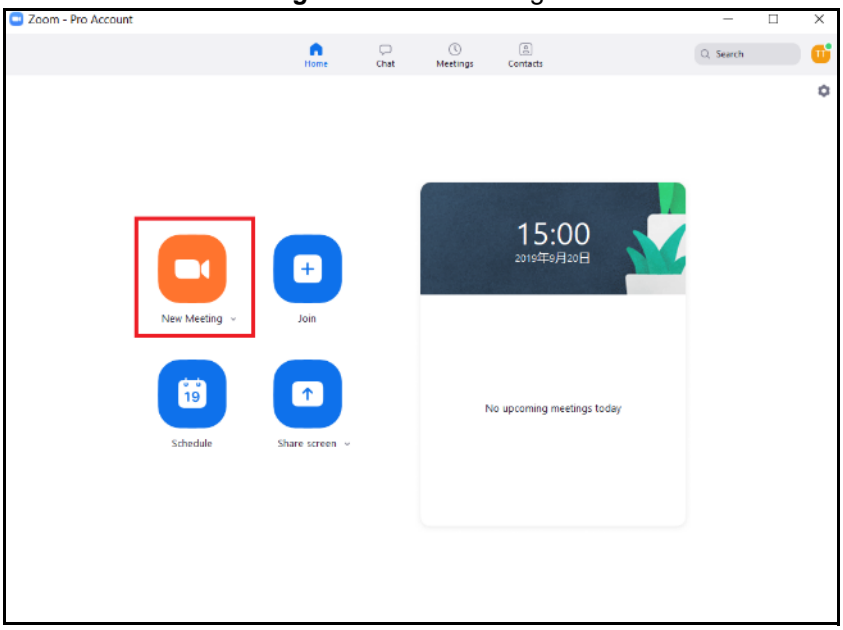
Topics:

Recording and Playback to Zoom meeting

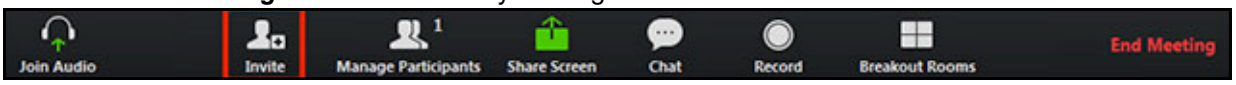
The HARMAN Media Suite only supports H323/SIP calls to Zoom conference.

1. Login to your Zoom account on your Zoom desktop application.

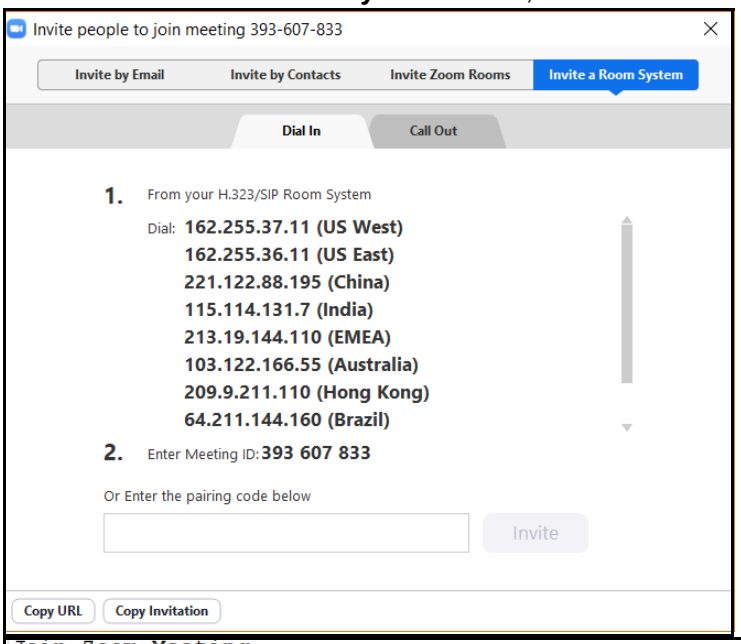
2 Click ***New meeting*** to start the meeting.



3 Get the ***meeting ID*** and ***Zoom IP*** by clicking on the icon **Invite**.



4 Select ***Invite a Room System*** toolbar, select the ***Dial In*** tab and then select ***Copy Invitation***




```
Join Zoom Meeting
https://zoom.us/j/393607833

One tap mobile
+493030806188,,393607833# Germany
+493056795800,,393607833# Germany

Dial by your location
        +49 30 3080 6188 Germany
        +49 30 5679 5800 Germany
        +49 69 7104 9922 Germany
        +1 929 436 2866 US (New York)
        +1 669 900 6833 US (San Jose)
Meeting ID: 393 607 833
Find your local number: https://zoom.us/u/acNJ3zjQA8

Join by SIP
393607833@zoomcrc.com

Join by H.323
162.255.37.11 (US West)
162.255.36.11 (US East)
221.122.88.195 (China)
115.114.131.7 (India)
213.19.144.110 (EMEA)
103.122.166.55 (Australia)
209.9.211.110 (Hong Kong)
64.211.144.160 (Brazil)
69.174.57.160 (Canada)
207.226.132.110 (Japan)
Meeting ID: 393 607 833
```

5 Dial from the HARMAN Media Suite side for Recording/Live/Playback.

- The full H.323 dial string format:

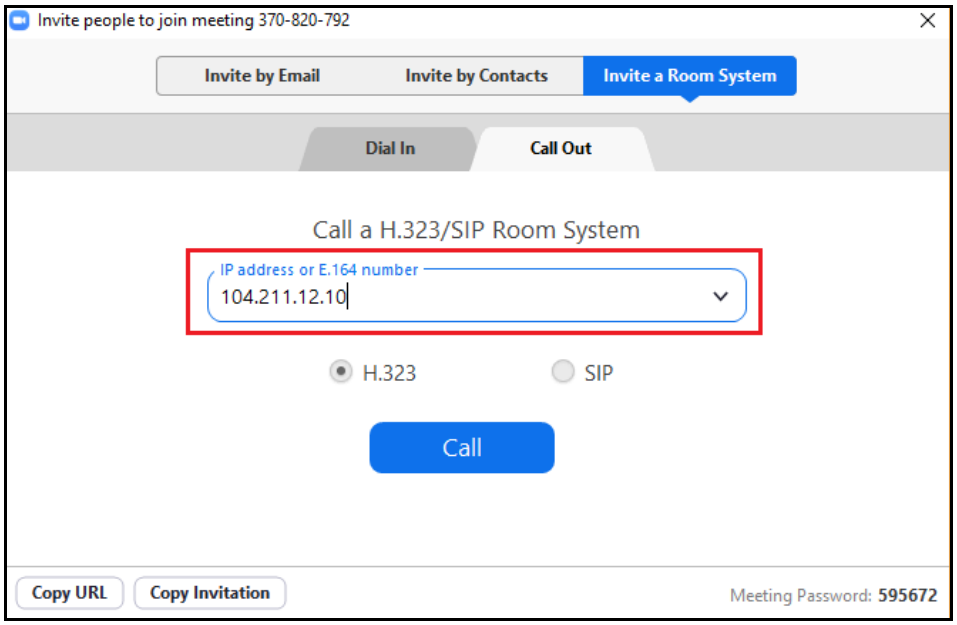
- ➢ Meetings without a password:
  [IP Address]##[Meeting ID] (Example: 192.168.1.25##123456789)
- ➢ Meetings with a password:
  [IP Address]##[Meeting ID]#[Password] (Example: 162.168.1.25##123456789#12345)

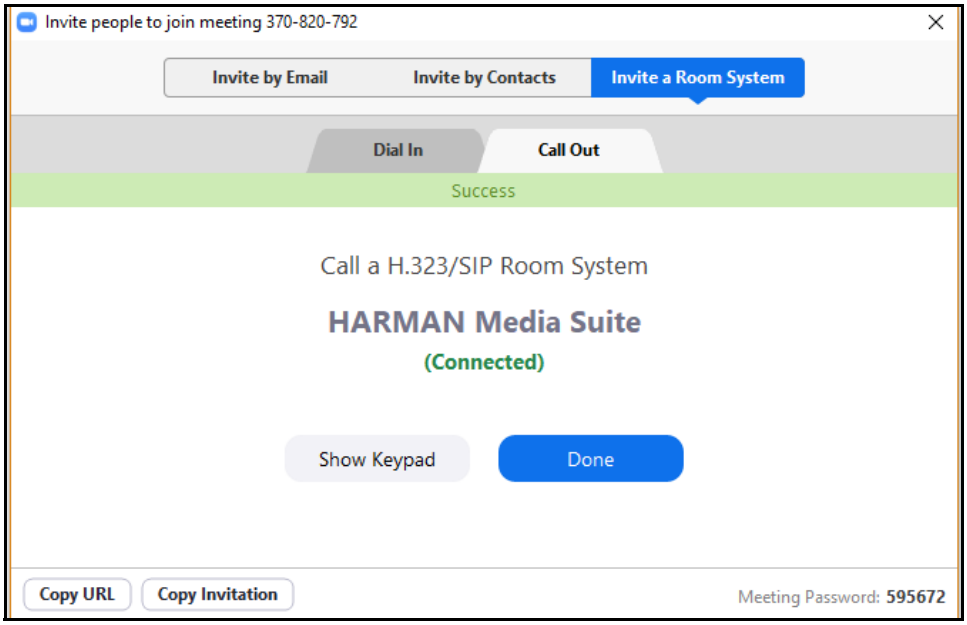
- The full SIP dial string format:
  - ➢ Meetings without a password:
    [Meeting ID]@[IP Address] (Example: 123456789@192.168.1.25)
    [Meeting ID]@zoomcrc.com (Example: 123456789@zoomcrc.com)
  - ➢ Meetings with a password:
    [Meeting ID].[Password]@[IP Address] (Example: 123456789.12345@192.168.1.25)
    [Meeting ID].[Password]@zoomcrc.com (Example: 123456789.12345@zoomcrc.com)

6 The call is established.

Zoom meeting call to the HARMAN Media Suite

1 Login your Zoom account on your Zoom desktop application.
2 Click **New meeting** to start the meeting.
3 Click the function icon **Invite**
4 Select Invite on the Zoom meeting toolbar, select the **Call Out**, enter the HARMAN Media Suite IP address.
5 Select the type of call you would wish to make - H.323 or SIP
6 Press **Call**.




Invite people to join meeting 370-820-792
Invite by Email
Invite by Contacts
Invite a Room System
Dial In
Call Out
Success
Call a H.323/SIP Room System
HARMAN Media Suite
(Connected)
Show Keypad
Done
Copy URL
Copy Invitation
Meeting Password: 595672

Appendix G– Configure HARMAN Media Suite LTI tool with LMS platform

Topics:

This chapter describes how to configure the HARMAN Media Suite while working with LMS platform such as Moodle and Sakai.

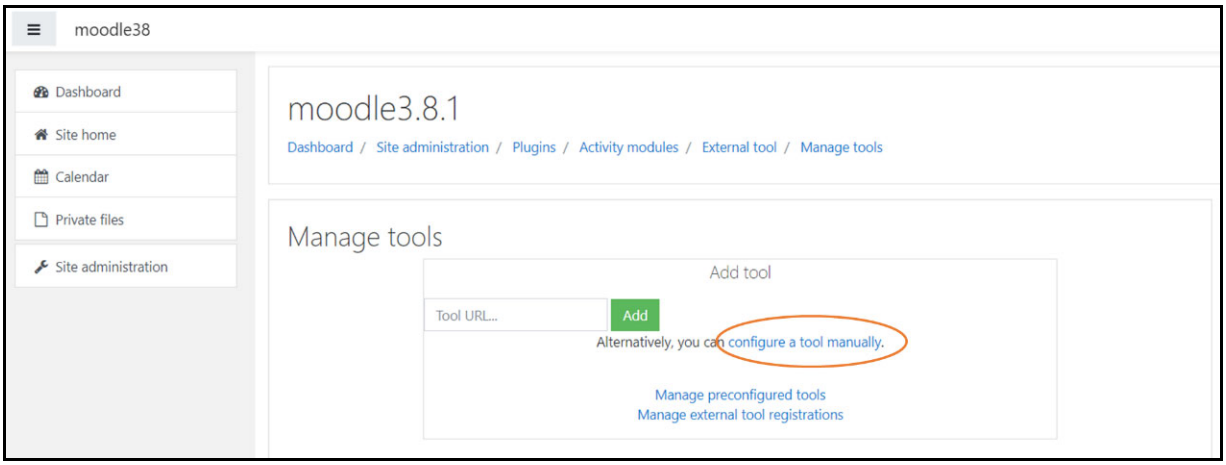
HTTPS must be used with a proper/trusted certificate for LTI integration.

Configure the HARMAN Media Suite LTI tool with Moodle

Create external tool of Moodle for the HARMAN Media Suite

Procedure

1. Login to **Moodle** with your Admin account credentials.
2. Enter **Site administration** > **Plugins** > **Manage tools**.
3. Click on **configure a tool manually**.

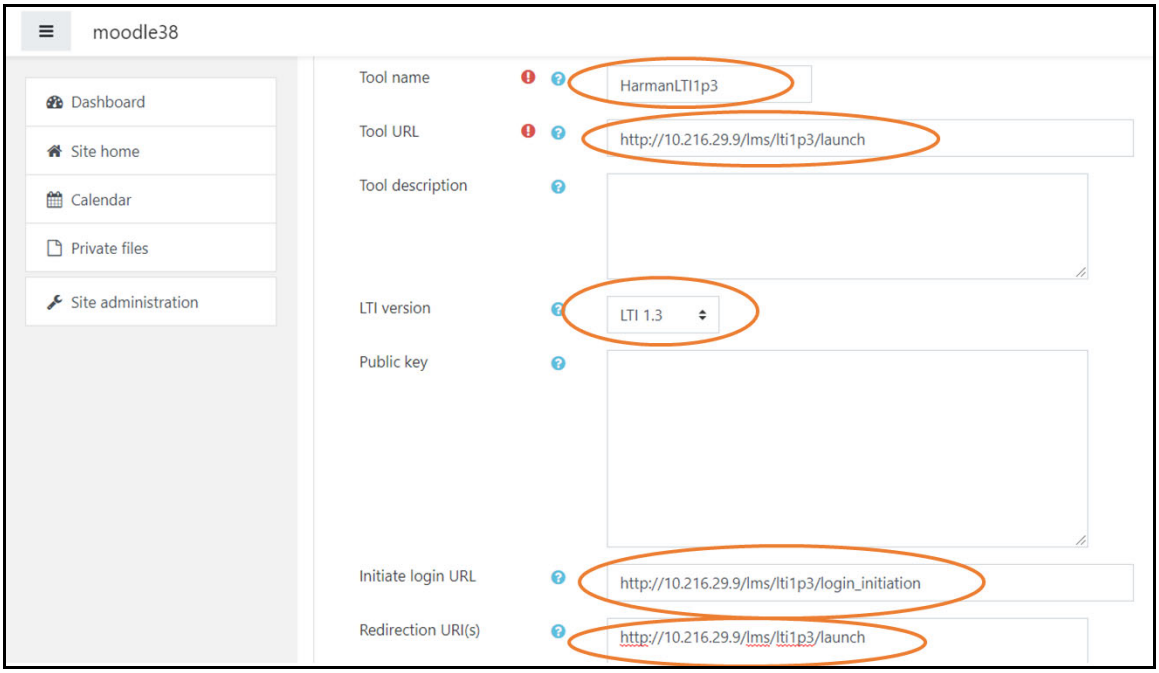


4. Enter necessary information for the external tool.

   For example, if the IP address of the HARMAN Media Suite system is 10.216.29.23

   - Tool name: **Specify the tool name**

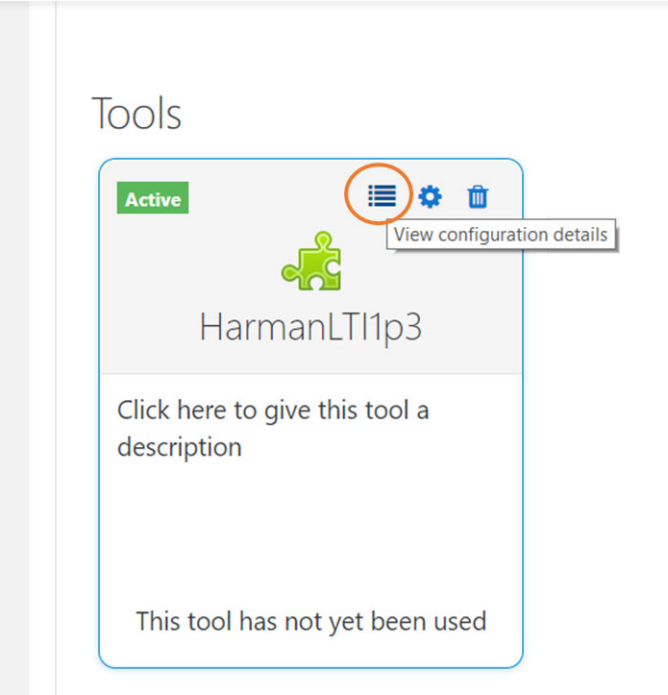
- Tool URL: **https://10.216.29.23/lms/lti1p3/launch**
- LTI version: **only support LTI 1.3**
- Initiate login URL: **https://10.216.29.23/lms/lti1p3/login_initiation**
- Redirection URI(s): **https://10.216.29.23/lms/lti1p3/launch**

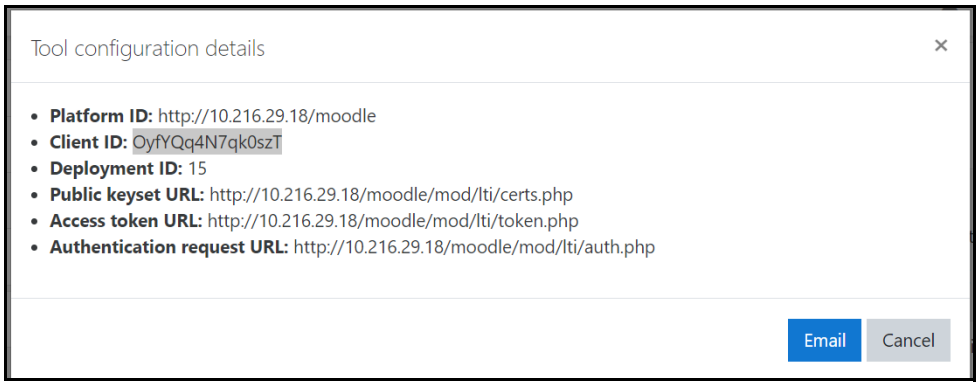


5 Click **Save changes** to create this external tool.

6 Click **View configuration details** icon to get the configuration details such as:

Platform ID, Client ID, Deployment ID, Public keyset URL, Access token URL, Authentication request URL





7 Generate the **LTI 1.3 Tool Public Key.**

Note: The HARMAN Media Suite must have LTI Support license.

a Launch the LTI Tool Registration page: **https://MediaSuiteIP/lms/lti1p3/registration**

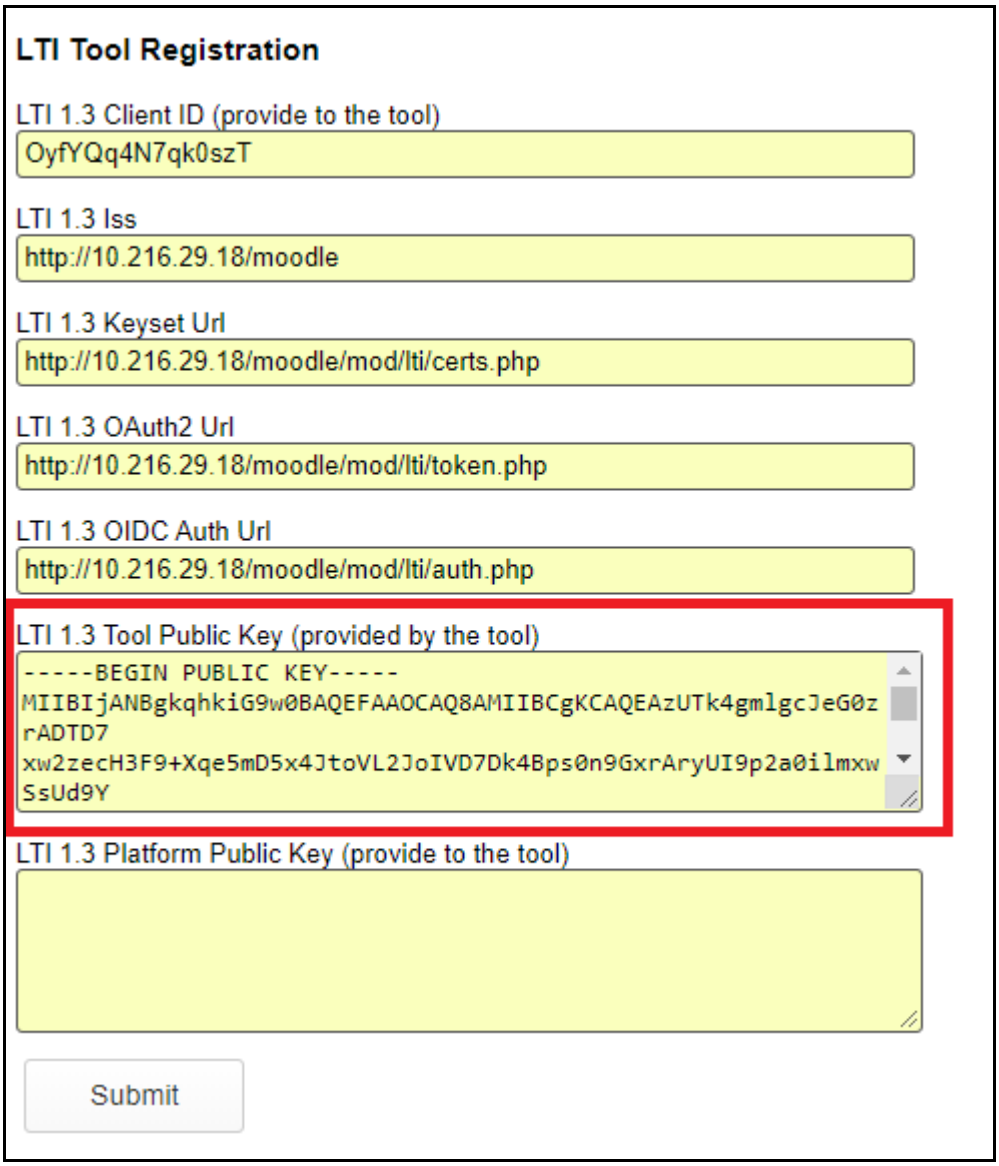
For example, if the IP address of the HARMAN Media Suite system is 10.1.2.3, launch the URL: https://10.1.2.3/lms/lti1p3/registration

b Enter the information in the corresponding fields.

- **LTI 1.3 Client ID:** Enter with **Client ID**
- **LTI 1.3 Iss**: Enter **Platform ID**

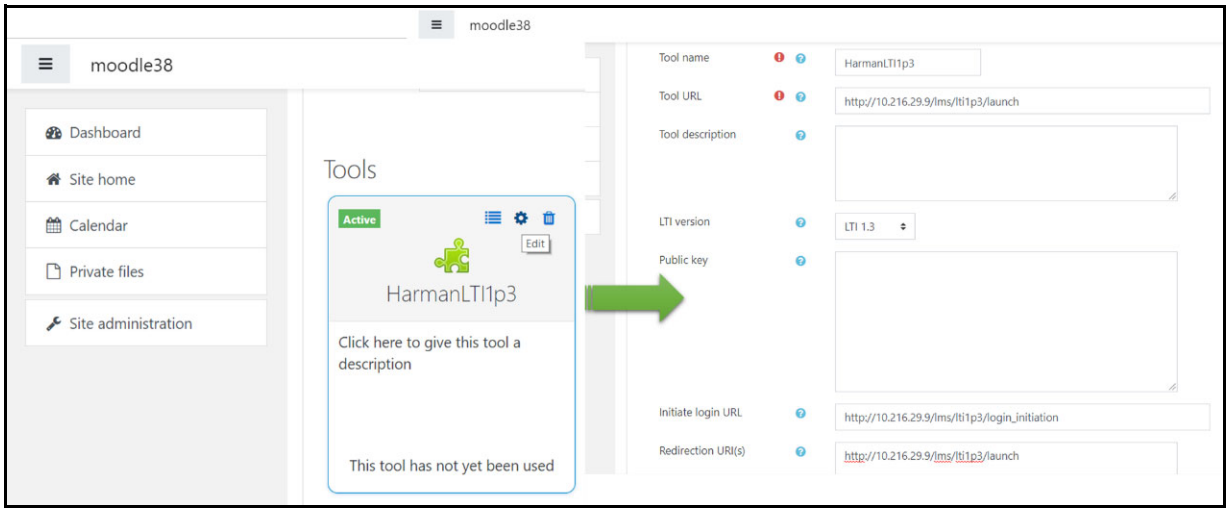
- **LTI 1.3 Keyset Url**: Enter with **Public keyset URL**
- **LTI 1.3 OAuth2 Url**: Enter with **Access token URL**
- **LTI 1.3 OIDC Auth Url:** Enter with **Authentication request URL**
- **LTI 1.3 Tool Public Key (provided by the tool)**
- **LTI 1.3 Platform Public Key (provided to the tool)**

c Click **Submit** to generate **LTI 1.3 Tool Public Key**.



8 Go to Moodle and edit the created external tool.

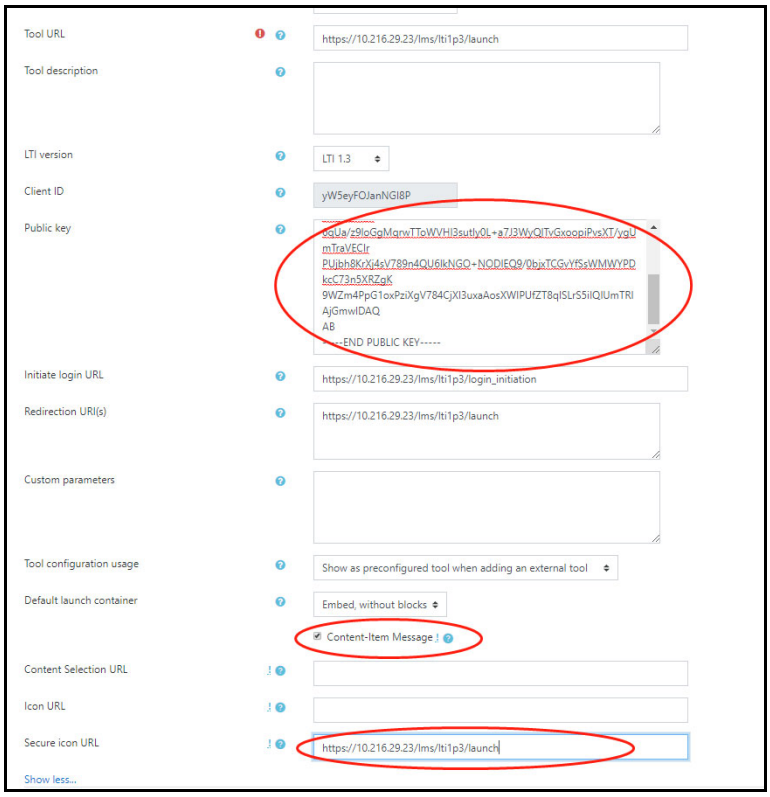
a Enter the **LTI 1.3 Tool Public Key to Public Key**.



b Enable **Content-Item Message**.

c Enter the **Secure icon URL**.

For example, if the IP address of the HARMAN Media Suite system is 10.216.29.23, launch URL: **https://10.216.29.23/lms/lti1p3/launch**

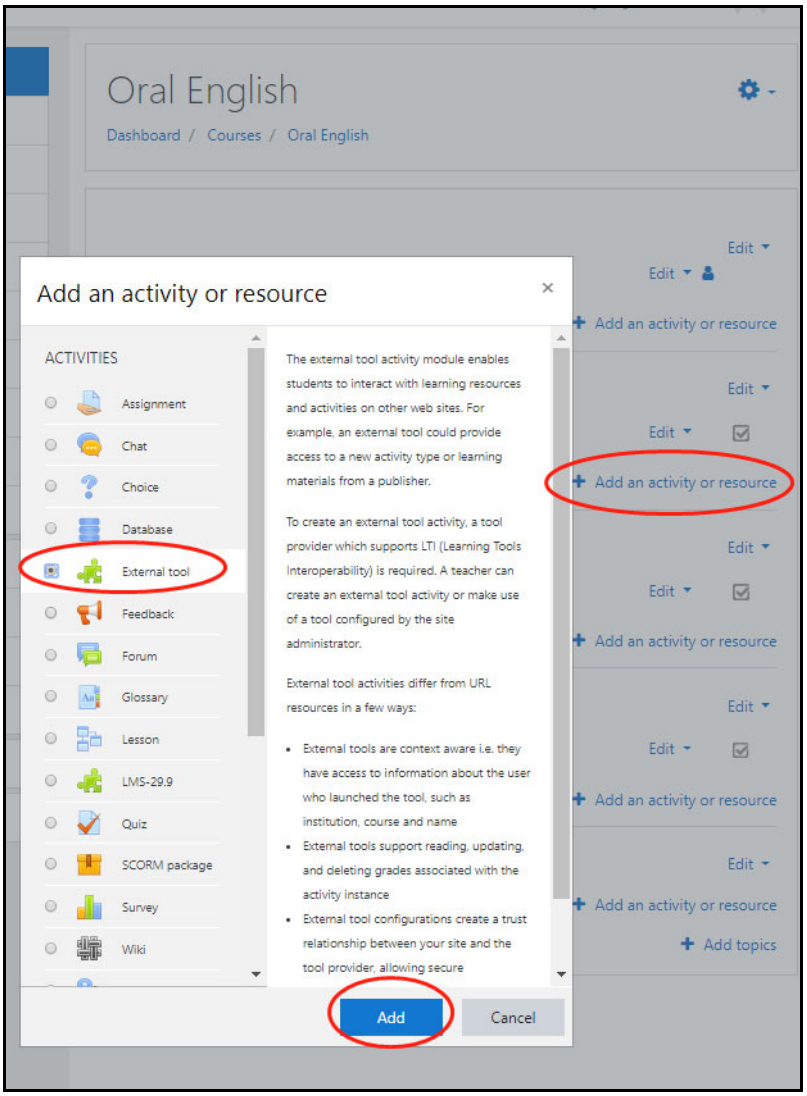


d Click **Save changes**

Add the media to Moodle course by Teacher

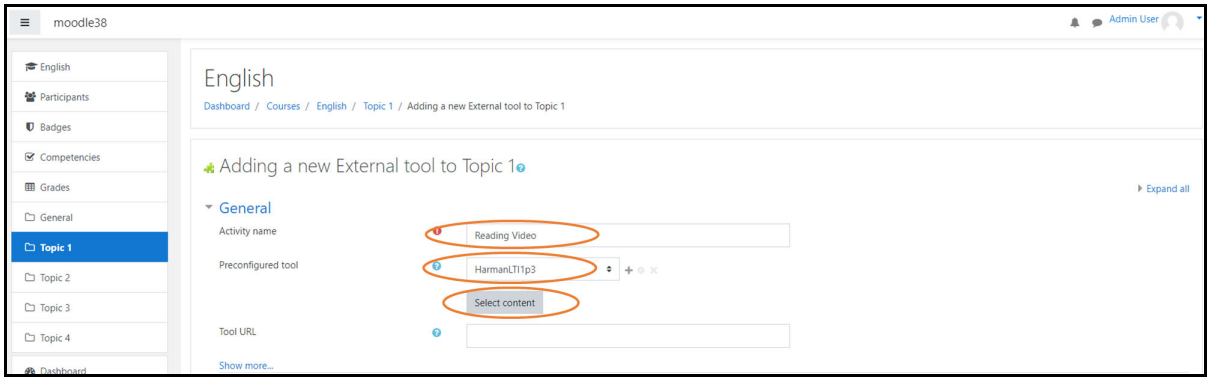
Procedure

1. Login to Moodle with the Teacher account credentials.
2. Choose and open desired courses.
3. Click on **Setting > Turn editing on**.
4. Add External tool
   a. Click **Add an activity or resource**
   b. Choose **External tool**
   c. Click **Add**

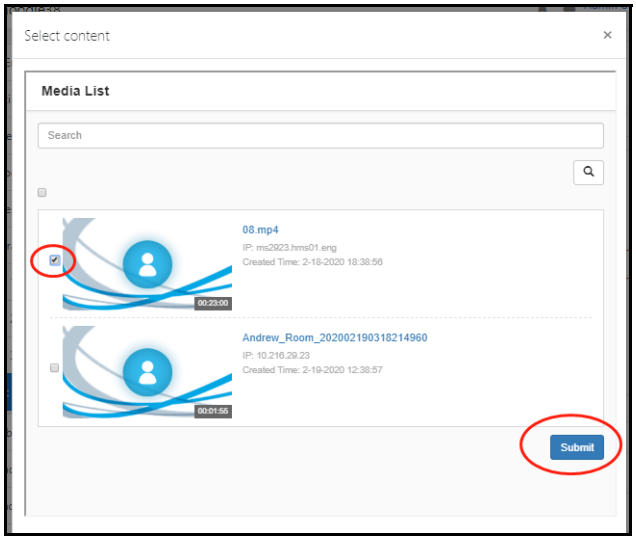


5. Enter name to **Activity name**.
6. Choose created HARMAN Media Suite LTI tool in **Preconfigured tool** list.

7 Click **Select Content**, the HARMAN Media Suite Media list page will appear.



8 Select desired media from the HARMAN Media Suite page and Click **Submit**.



Watch the media by Student

Procedure

1 Login to Moodle with the student account credentials.

2 Choose the course, which has already added the HARMAN Media Suite media from external tool.

3 Choose desired media in media list

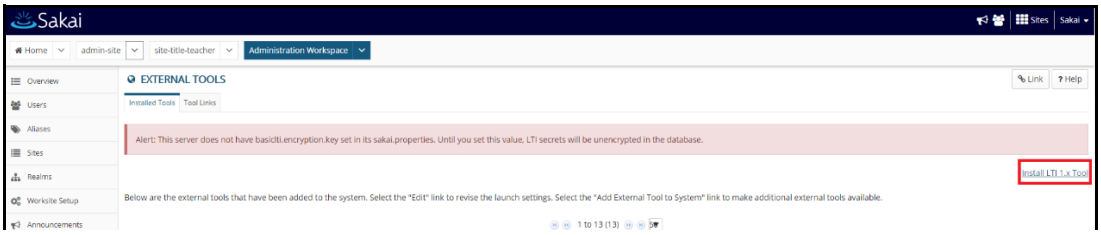
4 Click the **Play** button

Configure the HARMAN Media Suite LTI tool with Sakai

Create external tool of Sakai for the HARMAN Media Suite

Procedure

1. Login to Sakai with the admin account credentials
2. Go to **Worksite Setup** > **Administration Workspace**.
3. Select **External Tools**.
4. Click Install **LTI 1.x Tool** to add external tool.

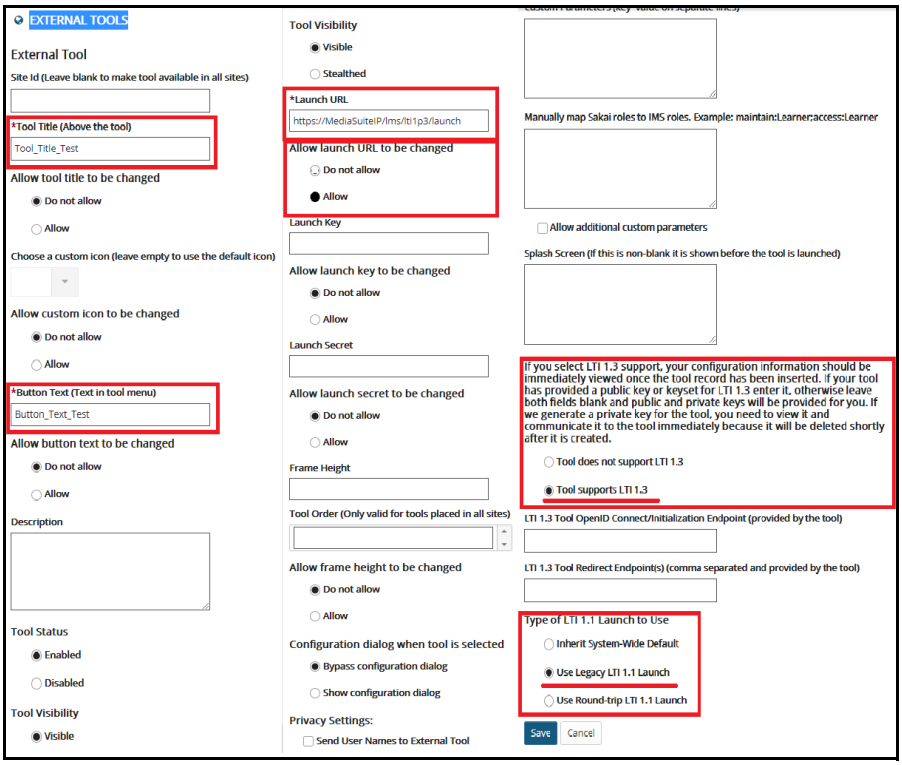


5. Enter necessary information for the external tool.
   a. Enter **Tool Title**, **Button Test**, launch URL.

   For example, if the IP address of the HARMAN Media Suite system is 10.1.2.3, Launch URL: https://10.1.2.3/lms/lti1p3/launch

   b. Enable **Tool Supports LTI1.3 and Use Legacy LTI 1.1 Launch** and Allow launch URL to be changed.

c Click **Save.**



6 Click on the created external tool to get below information.

- LTI 1.3 Client ID
- LTI 1.3 Platform OAuth2 Well-Known/KeySet URL
- LTI 1.3 Platform OAuth2 Bearer Token Retrieval URL
- LTI 1.3 Platform OIDC Authentication URL
- LTI 1.3 Issuer for this Platform

7 Generate the **LTI 1.3 Tool Public Key**.

Note: The HARMAN Media Suite must have **LTI Support** license.

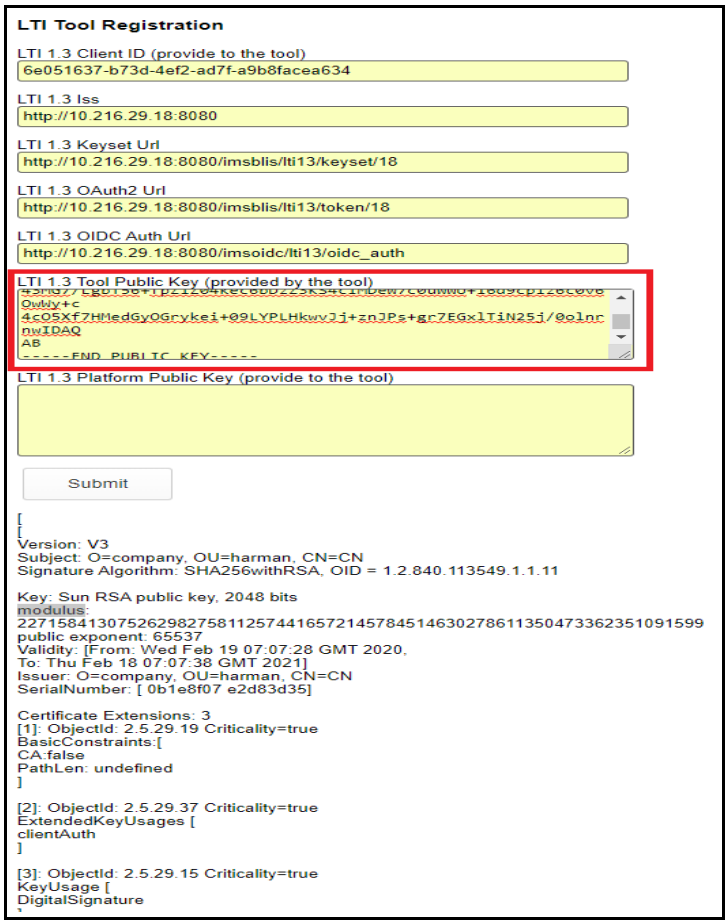
a Launch the **LTI Tool Registration** page: https://MediaSuiteIP/lms/lti1p3/registration

For example, if the IP address of the HARMAN Media Suite system is 10.1.2.3, launch the URL: **https://10.1.2.3/lms/lti1p3/registration**

b Enter the information in the corresponding fields.

- **LTI 1.3 Client ID**: Enter with **LTI 1.3 Client ID**
- **LTI 1.3 Iss**: Enter with **LTI 1.3 Issuer for this Platform**
- **LTI 1.3 Keyset Url**: Enter with **LTI 1.3 Platform OAuth2 Well-Known/KeySet URL**
- **LTI 1.3 OAuth2 Url**: Enter with **LTI 1.3 Platform OAuth2 Bearer Token Retrieval URL**
- **LTI 1.3 OIDC Auth Url**: Enter with LTI 1.3 Platform OIDC Authentication URL

c Click **Submit** to generate LTI 1.3 Tool Public Key.



8 Go to Sakai and Edit the created external tool.

a Enter **LTI 1.3 Tool Public Key (provided by the tool)**.

b Delete **LTI 1.3 Tool Private Key (for messages from the tool)**.

c Enter **LTI 1.3 Tool OpenID Connect/Initialization Endpoint**.

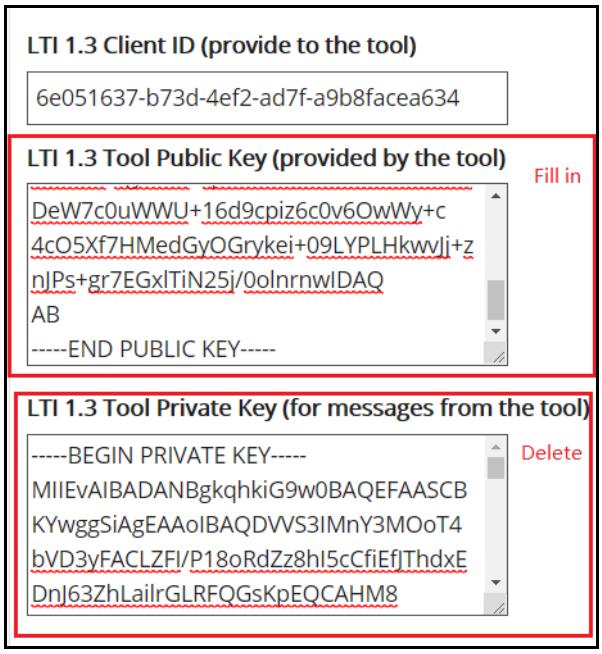
d Enter **LTI Tool Registration URL**: **https://MediaSuite/lms/lti1p3/login_initiation**

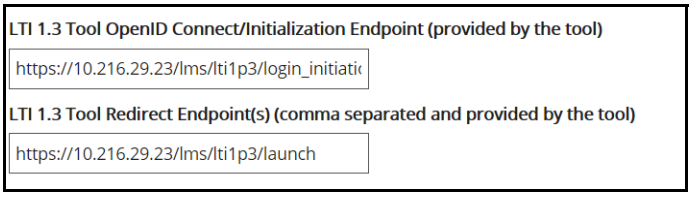
For example, if the IP address of the HARMAN Media Suite system is 10.216.29.23, launch URL: **https://10.216.29.23/lms/lti1p3/login_initiation**

e Enter **LTI 1.3 Tool Redirect Endpoint(s)** URL: https://MediaSuite/lms/lti1p3/launch

For example, if the IP address of the HARMAN Media Suite system is 10.216.29.23, Launch URL: **https://10.216.29.23/lms/lti1p3/launch**

f Click **Save**.





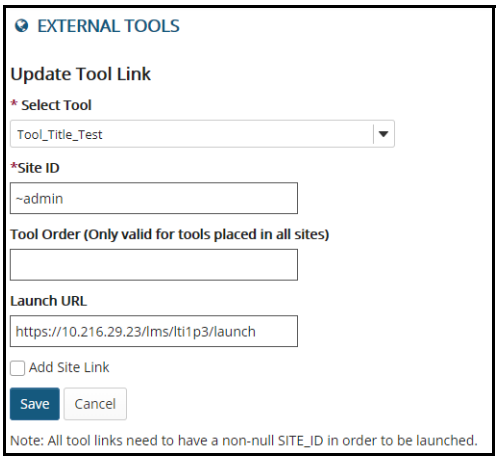
Create Tool Link

Procedure

1. Login to Sakai with the admin account credentials.
2. Click **Worksite Setup > Administration Workspace > External Tools**.
3. Click **Tool Links > Create Tool Link** to add new tool link.
4. Choose correct external tool from **Select Tool**.
5. Enter name to **Site ID**.
6. Enter correct launch URL.

   URL: **https://MediaSuite/lms/lti1p3/launch**

   For example, if the IP address of the HARMAN Media Suite system is 10.216.29.23, Launch URL: **https://10.216.29.23/lms/lti1p3/launch**
7. Click **Save**.



Enter Tool Link

Procedure

1. Login to Sakai.
2. Click **Worksite Setup > Administration Workspace > External Tools**.
3. Click **Tool Links** Tab.
4. Choose correct tool link and Click the **URL**.
5. Click the **Process with LTI 1.3 Launch** button to login.

Appendix H– Configure SAFR Server for Facial Recognition

Topics:

- Configure SAFR Server for Facial Recognition

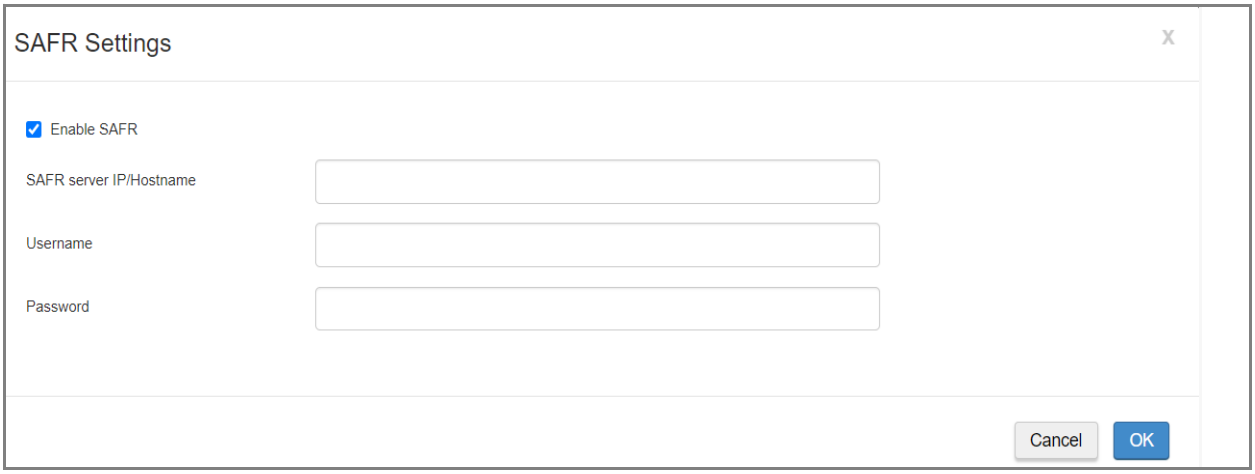
This chapter describes how to configure the SAFR Server for Facial Recognition.

Configure SAFR Server for Facial Recognition

The SAFR Facial Recognition service in HARMAN Media Suite is available only with the purchase of **Platinum** license. In order to use the SAFR facial recognition service with HARMAN Media Suite, it is required to do mandatory configuration in the admin portal.

Procedure

1. Navigate to **Configuration** > **SAFR Settings.**
2. In **SAFR Settings** form, select the option **Enable SAFR.**
3. Fill the details as shown below and click **OK**.



The confirmation message appears once you enter correct credentials otherwise error message appears.

Depending on the archives in customer's database, specific users are required to search, which are created by the admin users in the admin portal. Select a desired role and upload the profile picture of good quality. For more information, refer to User and Group Management.

Appendix I– Configure the SSO via SAML on the IdP side

Topics:

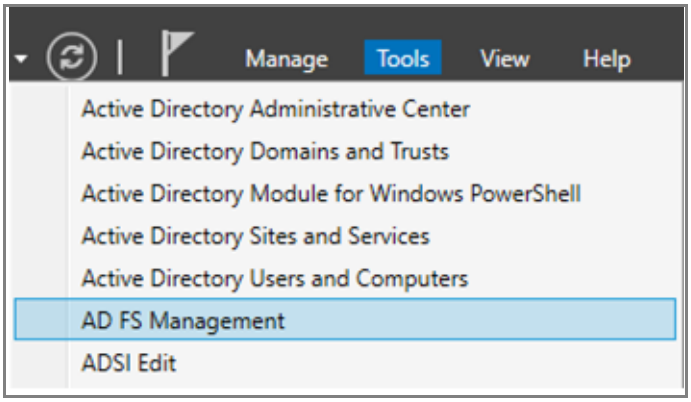
- Configure ADFS for supporting SSO login via SAML

This chapter describes how to configure the SSO via SAML on the IdP side.

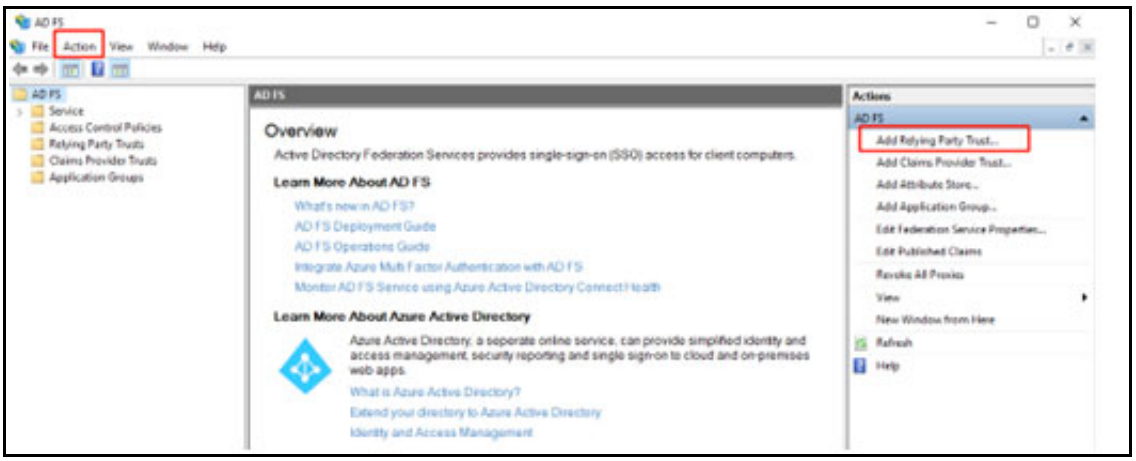
Configure ADFS for supporting SSO login via SAML

Procedure

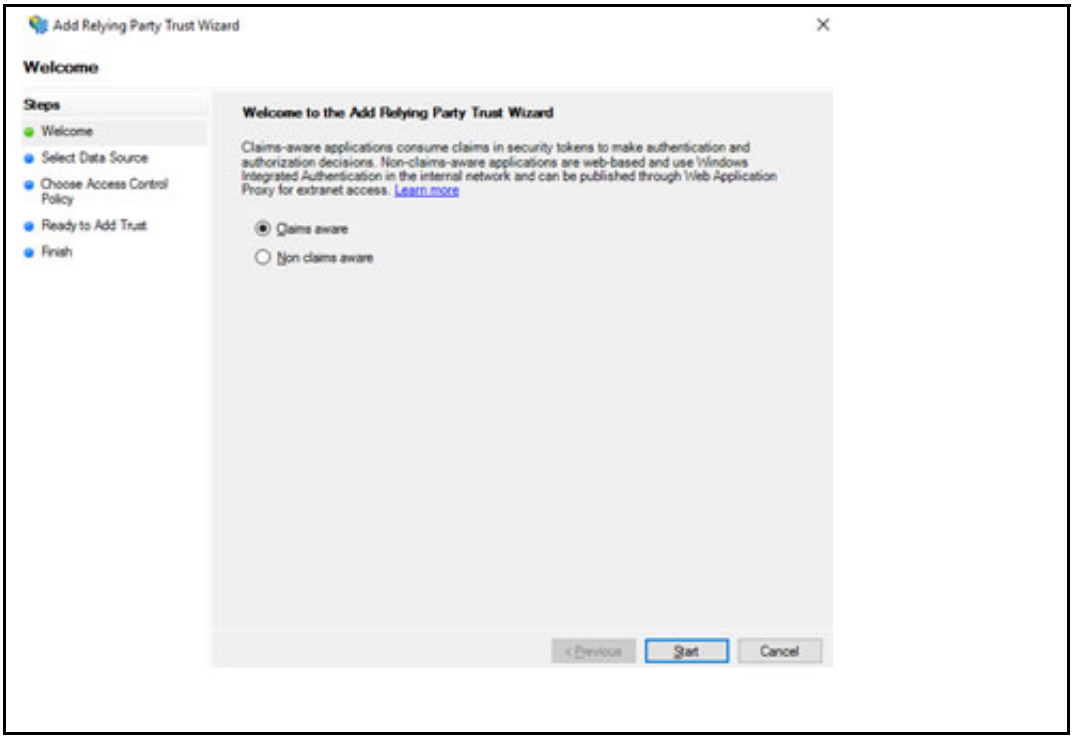
1 In the Windows server, which enabled the ADFS service, click **Tools** > **AD FS Management.**



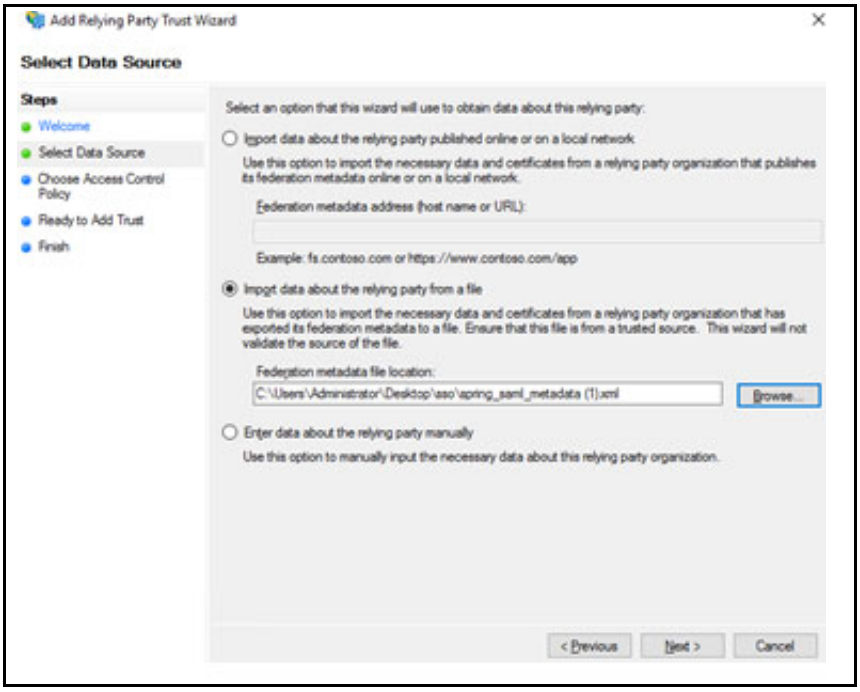
2 Click **Add Relying Party Trust** in the sidebar of the **Actions** menu.



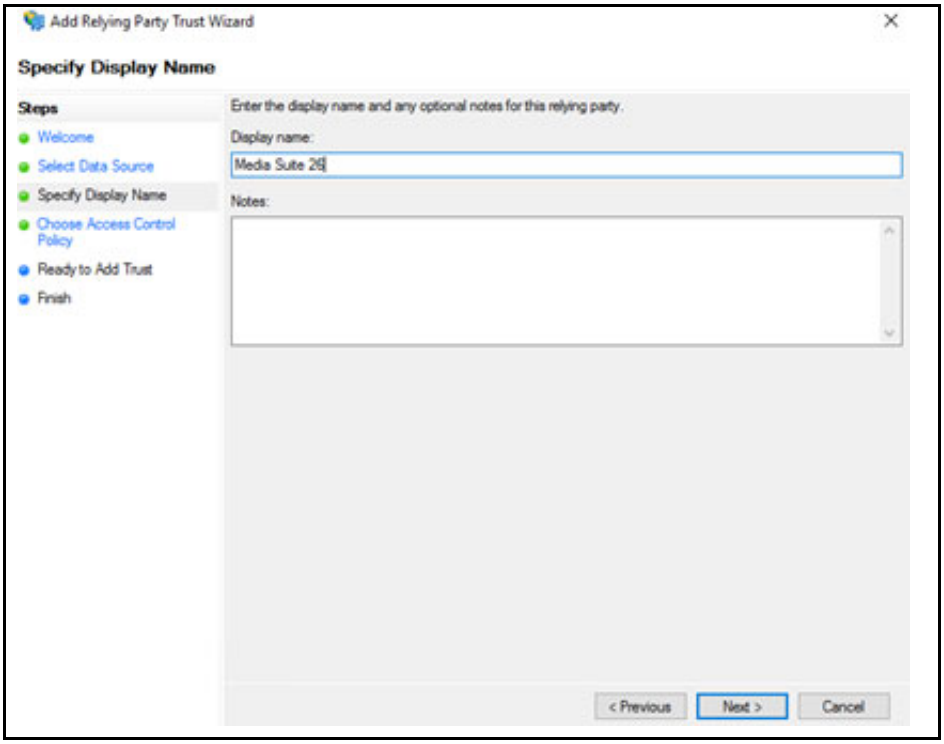
3 In the **Wizard**, select **Claims aware** as the default option, Click **Start.**



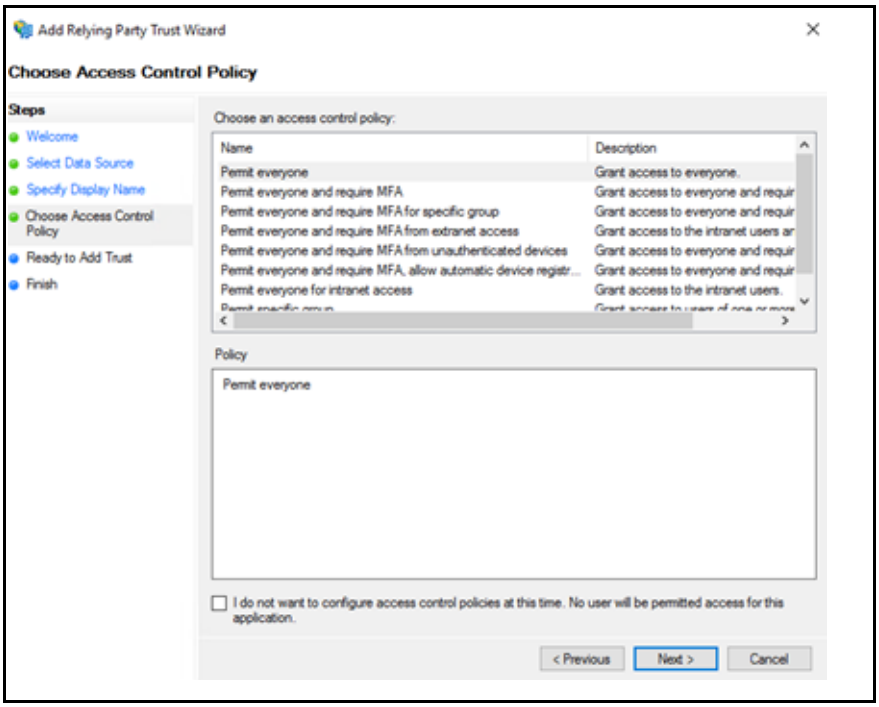
4 Choose **Import data about the relying party from a file** and go to select the metadata.xml which we downloaded from **Media Suite.**



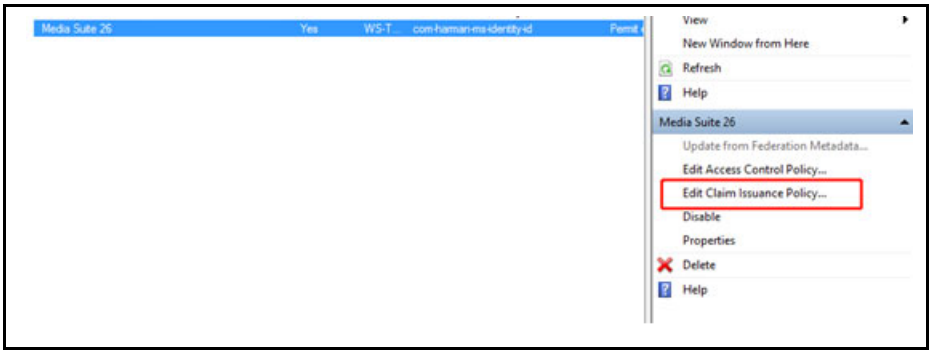
5 Input any Display name and Notes of your application, here is for **Media Suite**, Click **Next**.



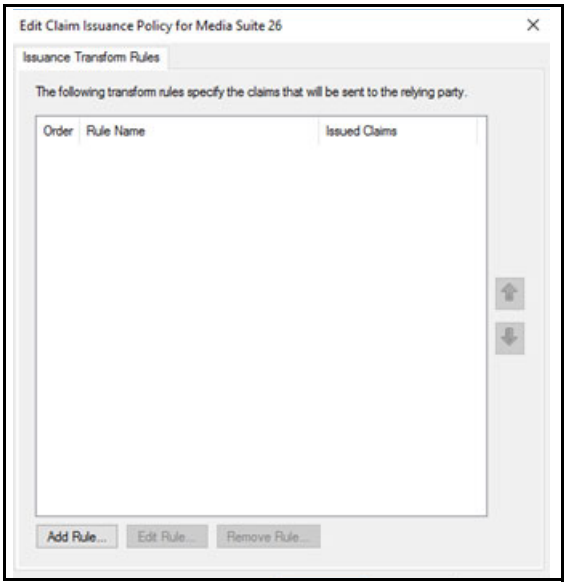
6 Select the **Permit everyone** as the default option and click **Next** until finish the Wizard.



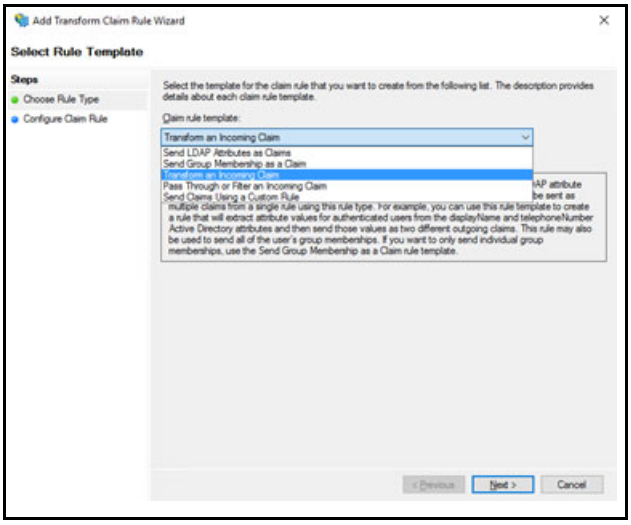
7 Select the newly created Item, Click **Edit Claim Issuance Policy.**



8 Click **Add Rule**.



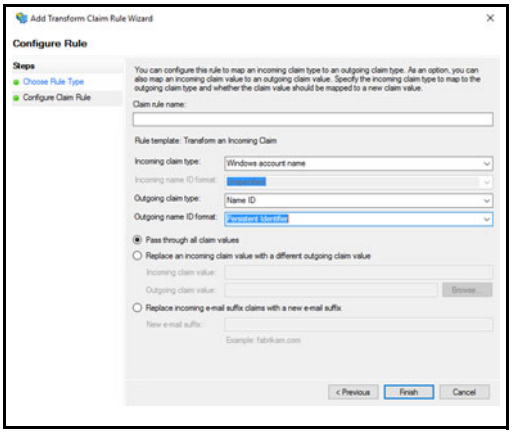
9 Select **Transform an Incoming Claim** and click **Next.**



10 Input desired rule name under **Claim rule name**,

- **a** Select the **Windows account name** for I**ncoming claim type**
- **b** Select the **Name ID** for **Outgoing claim type**
- **c** Select the **Persistent Identifier** for **Outgoing name ID format**

11 Click the **Finish** button.



After the configuration, your application will appear under your ADFS web portal.
https://[Host]/adfs/ls/idpinitiatedsignon.aspx.

Appendix J– Configure the AI Based Services

Topics:

This chapter describes how to configure different AI Based Services in the AWS cloud.

Configure the AWS for supporting Transcription Service

Prepare the S3 bucket with the necessary files and template provided by HARMAN

We need the files and template to create the CloudFormation stack and S3 bucket to support the transcription service on AWS.

If you already have an S3 bucket, you can use it to upload those files in step 4.

Procedure

1. Log in to **S3 Management Console**.
2. Create an **S3 bucket**.
   a. Click **Create bucket** button.
   b. Input the desired **Bucket name**, choose the desired **AWS Region** and then click **Create bucket** button to finish the creation.
3. Under **Amazon S3** > **Buckets**, find your new created **S3 Bucket** and click to enter it.
4. Upload the **ms_transcribe_s3_file.zip**, **ParseJsonToSrt.zip** and **s3-lambda-transcribe-template-v1.yaml** into your bucket. You can get these files from **HARMAN SUPPORT TEAM**, please contact HCS-CustomerSupport@harman.com

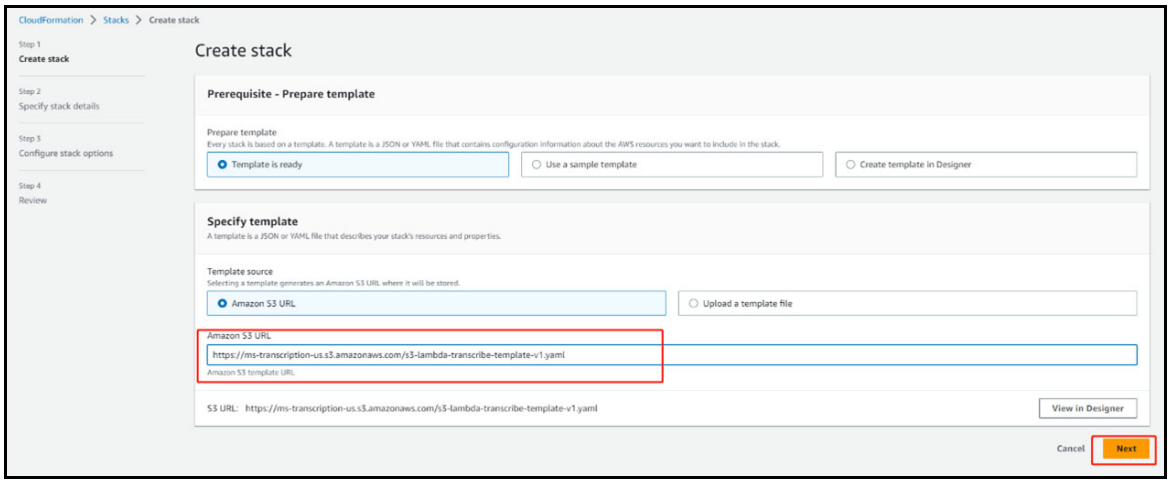
Create CloudFormation Stack

Procedure

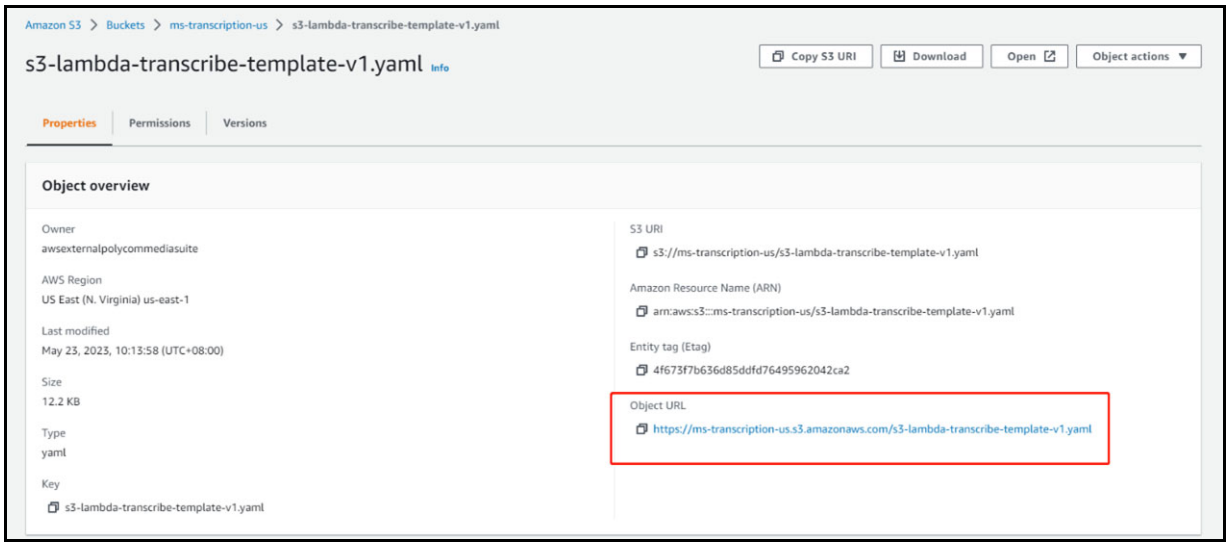
1. Log in to **CloudFormation Console**.
2. Select the same region at the right of the top bar as the **S3 bucket** you just created.

3 Click **Create stack** and select **With new resource (standard)** in the drop down list,

4 Fill the **Amazon S3 URL** with the URL of the **s3-lambda-transcribe-template-v1.yaml** you just uploaded on your S3 Bucket and click the **Next** button,



You can find the URL under **S3** > **buckets** > **your bucket**, click on the **s3-lambda-transcribe-template-v1.yaml** and copy the **Object URL**.



5 Specify your desired name for **Stack name** and **MSBucketName**.

6 Fill the **SourceBucket** with your S3 bucket name and click the **Next** button.

7 Keep clicking the **Next** button and click **Submit** button to finish the creation.

8 When the stack is created successfully, go to **CloudFormation** > **Stacks**, enter your created stack and click the **Outputs** tab. You will find the required information by **Media Suite Transcription Settings**.

Configure the AWS for supporting Advanced Search Service

We need to configure the OpenSearch domain and API proxy server on AWS to support Advanced Search Service in HARMAN Media Suite.

Configure the AWS OpenSearch domain

Procedure

1 Log in to the **AWS OpenSearch Console.**
Please choose the region you desire to deploy.

2 Click the **Create domain** button to enter the domain configuration page.

3 Configure each option according to your requirements.

- HARMAN Media Suite only supports Create master user method under the Fine-grained access control tab now.
- Please note down the Master username and the Master password which will be used for the Media Suite Advanced Search Service configuration.
- HARMAN Media Suite supports the latest OpenSearch_2.5 now.

4 Click the **Create** button.

5 Wait for some time to have your OpenSearch domain **Active**.

6 Go to A**mazon OpenSearch Service** > **Domain** > **your domain**, you can find the **Domain endpoint** information in the **General Information** tab which will be used for the **Media Suite Advanced Search Service** configuration.

Configure the API proxy server by the AMI shared from HARMAN

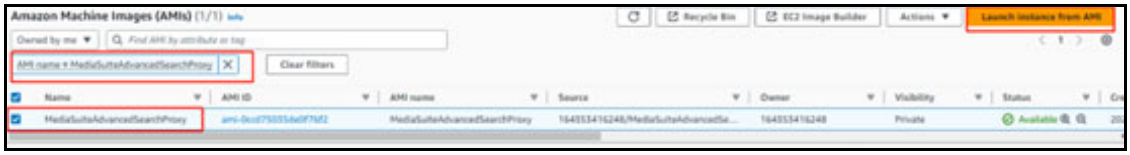
The customer who is going to use Advanced Search Service needs to ask HARMAN CUSTOMER SUPPORT (HCS-CustomerSupport@harman.com) to share the AMI by providing **AWS Account ID** and preferred **Region**, then the customer can follow the procedure to set up the API proxy server.

Procedure

1 Log in to the **EC2 Management Console**. Please choose the region you desire to deploy.

2 Click **Images** > **AMIs** in the left sidebar.

3 Search the AMI by the name "**MediaSuiteAdvancedSearchProxy**", check it and click **Launch instance from AMI.**



4 Configure each option according to your requirements:

- The recommended instance type is t**2.2xlarge** and the minimum requirement is 8 cores for CPU and 16 GiB for Memory.
- The minimum requirement for storage is 50 GiB.

5 Check the information in **Summary** and click the **Launch instance** button.

6 After the instance is running normally, you can get the IPv4 address used for the **Media Suite Advanced Search Service** configuration.