



HAIVISION

Haivision Media Platform 3.5
Administrator's Guide

HVS-ID-AG-HMP-35

Edition Notice

© 2015-2023 Haivision. All rights reserved.

This edition and the products it describes contain proprietary and confidential information. No part of this content may be copied, photocopied, reproduced, translated or reduced to any electronic or machine-readable format without prior written permission of Haivision. If this content is distributed with software that includes an end-user agreement, this content and the software described in it, are furnished under license and may be used or copied only in accordance with the terms of that license. Except as permitted by any such license, no part of this content may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Haivision Systems, Inc. Please note that the content is protected under copyright law even if it is not distributed with software that includes an end-user license agreement.

About Haivision

Founded in 2004, Haivision is now a market leader in enterprise video and video streaming technologies. We help the world's top organizations communicate, collaborate and educate. Recognized as one of the most influential companies in video by Streaming Media and one of the fastest growing companies by Deloitte's Technology Fast 500, organizations big and small rely on Haivision solutions to deliver video. Headquartered in Montreal, Canada, and Chicago, USA, we support our global customers with regional offices located throughout the United States, Europe, Asia and South America.

Trademarks

The Haivision logo, Haivision, and certain other marks are trademarks of Haivision. CoolSign is a registered trademark licensed to Haivision Systems, Inc. All other brand or product names identified in this document are trademarks or registered trademarks of their respective companies or organizations.

Disclaimer

The information contained herein is subject to change without notice. Haivision assumes no responsibility for any damages arising from the use of this content, including but not limited to, lost revenue, lost data, claims by third parties, or other damages.

If you have comments or suggestions, please contact infodev@haivision.com.

While every effort has been made to provide accurate and timely information regarding this product and its use, Haivision Systems Inc. shall not be liable for errors or omissions contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Contents

Edition Notice	2
About Haivision	2
Trademarks	2
Disclaimer	2
Contents	3
About This Document	6
Conventions	6
Typographic Conventions and Elements	6
Action Alerts.....	6
Obtaining Documentation.....	7
Getting Service Support	7
Introduction	8
Product Editions	9
Enterprise Edition.....	9
Workgroup Edition	10
Product Features	10
Multicast Support via Haivision Helper and Multicast Agent.....	13
HMP-Media Gateway Pairing.....	14
SRT (Secure Reliable Transport).....	15
High Availability Clustering Failover Support	15
Getting Started	17
Accessing the HMP Web Interface	17
SSL Encryption	19
Changing the Default Password	19
Navigating the Interface	20
Modifying the IP Address	20
Creating a New Admin User.....	22
Adding a Source	23
Configuring HMP	25
Adding Export Destinations.....	25
Export Destination Settings	27
Configuring Feeds and Activating the Portal.....	28
Configuring IPTV Channels.....	30
Changing IPTV Channel Numbers.....	31
Configuring Locations	38
Multicast Playback.....	38
Managing Locations.....	40
Location Settings.....	42
Locations Topology	45
Locations Policies.....	47
Troubleshooting Multicast and Diagnostic Tool	49
Pairing Media Gateways to HMP.....	51
Configuring Multi-Site Live Distribution	53
Defining Metadata	59
Metadata Settings	63
Managing KLV Inputs.....	63
Setting Default Set-Top Box Values	64
Device Default Settings.....	66

Tagging Devices.....	67
Managing Sources	68
Adding and Editing Sources	70
Creating a Watermark for a Source	72
Source Settings	75
Configuring Secure Reliable Transport (SRT) Sources	79
Managing Stream Outputs.....	80
Re-Branding the User Interface	81
User Interface Settings.....	82
Configuring Video and Session Settings.....	84
Using an External Player to View Sessions	84
Adjusting STB Player Tuning	85
Managing Access Controls	87
Managing Users	87
Assigning Roles to LDAP/AD Users.....	89
Managing User Accounts (Non LDAP/AD)	90
User Settings	91
Managing Groups (LDAP/AD Only).....	92
Assigning Roles to LDAP/AD Groups	94
Managing Roles	95
Adding Users and Groups to Roles	96
Editing Role Permissions	97
Creating Custom Roles.....	99
Default Roles	100
Customizing the Navigation Toolbar for Each Role	102
Managing Access Permissions.....	103
Managing System Settings	106
Activating Command Line API Access	106
Backing Up and Restoring HMP.....	107
Backing Up HMP	109
Uploading Backup Files.....	112
Restore to a Previous Configuration.....	112
Backup/Restore Settings	114
Managing Certificates	115
Generating a Certificate Signing Request (CSR).....	115
Importing and Activating a Certificate (CRT).....	116
Generating a Private Key.....	118
Importing a Private Key	119
Generating a New Self-Signed Certificate.....	120
Certificate Settings	120
Managing Directory (Authentication) Services	122
Connecting to a Directory Server	122
Disconnecting from a Directory Server	125
Directory Service Settings	125
Integrating HMP with Single Sign-On (SSO) Environments.....	127
Single Sign-On (SSO) Settings.....	130
Licensing Your HMP.....	134
Configuring Network Settings.....	136
Network Settings	138
Managing Network Storage.....	141
Configuring Watch Folders	142
Formatting XML Data to Import into HMP with Media Files	143
Importing Custom EPG Data into HMP.....	145
Managing Security.....	147
Configuring Appliance Security.....	148
Security Settings.....	150
Installing System Updates.....	154
Reverting an Upgrade.....	156
Reporting	158
Reports and Logs	159
Viewing System Activity.....	161

Viewing High Availability Cluster Status.....	163
KLV Dictionary Format	164
Dictionary Syntax	164
Item - Translation.....	164
Item - Translation/Format/Suffix/Precision	165
Item - Enum.....	166
64-bit Integer.....	169
Technical Specifications	170
Haivision Media Platform Software	170
Haivision Media Platform Hardware	171
Warranties	172
1-Year Limited Hardware Warranty	172
EXCLUSIONS AND LIMITATIONS	172
OBTAINING WARRANTY SERVICE.....	173
APPLICABLE LAW	173
EULA - End User License Agreement.....	174
READ BEFORE USING	174
SLA - Service Level Agreement.....	174
1. Introduction.....	174
2. Definitions	174
3. Service Levels for the Video Content Management System	174
4. Exceptions to Availability for the VCMS	175
5. Credits for Downtime for the VCMS.....	176
6. Support Services for the VCMS	176
7. Service Levels for Haivision Streaming Media Service	177
8. Credits for Outages of Haivision Streaming Media Service.....	177
9. No Secondary End User Support	177
Getting Help	178

About This Document

Conventions


The following conventions are used to help clarify the content.

Typographic Conventions and Elements


<i>Italics</i>	Used for the introduction of new terminology, for words being used in a different context, and for placeholder or variable text.
bold	Used for strong emphasis and items that you click, such as buttons.
Monospaced	Used for code examples, command names, options, responses, error messages, and to indicate text that you enter.
>	In addition to a math symbol, it is used to indicate a submenu. For instance, File > New where you would select the New option from the File menu.
...	Indicates that text is being omitted for brevity.

Action Alerts


The following alerts are used to advise and counsel that special actions should be taken.

 **Tip**

Indicates highlights, suggestions, or helpful hints.

 **Note**

Indicates a note containing special instructions or information that may apply only in special cases.

 **Important**

Indicates an emphasized note. It provides information that you should be particularly aware of in order to complete a task and that should not be disregarded. This alert is typically used to prevent loss of data.

⚠ Caution

Indicates a potentially hazardous situation which, if not avoided, may result in damage to data or equipment. It may also be used to alert against unsafe practices.

⚠ Warning

Indicates a potentially hazardous situation that may result in physical harm to the user.

Obtaining Documentation

This document was generated from the Haivision InfoCenter. To ensure you are reading the most up-to-date version of this content, access the documentation online at <https://doc.haivision.com>. You may generate a PDF at any time of the current content. See the footer of the page for the date it was generated.

Getting Service Support

For more information regarding service programs, training courses, or for assistance with your support requirements, contact Haivision Technical Support using our Support Portal at: <https://support.haivision.com>.

Introduction

This guide explains how to set up, configure, and manage Haivision Media Platform (HMP) systems.

Note

The intended audience for this guide is system integrators and administrators with administrative privileges.

For information on options available to non-administrative users, such as browsing content, working with sessions and videos, managing Portal content, and managing imports and exports, please refer to the Haivision Media Platform [User's Guide](#).

Note

HMP capabilities vary by product edition (Workgroup or Enterprise). Some features mentioned in this guide may not be available on your system. For more information, see [Product Editions](#).

Topics Discussed

- [Product Editions](#)
- [Product Features](#)
- [Multicast Support via Haivision Helper and Multicast Agent](#)
- [HMP-Media Gateway Pairing](#)
- [SRT \(Secure Reliable Transport\)](#)
- [High Availability Clustering Failover Support](#)

Product Editions

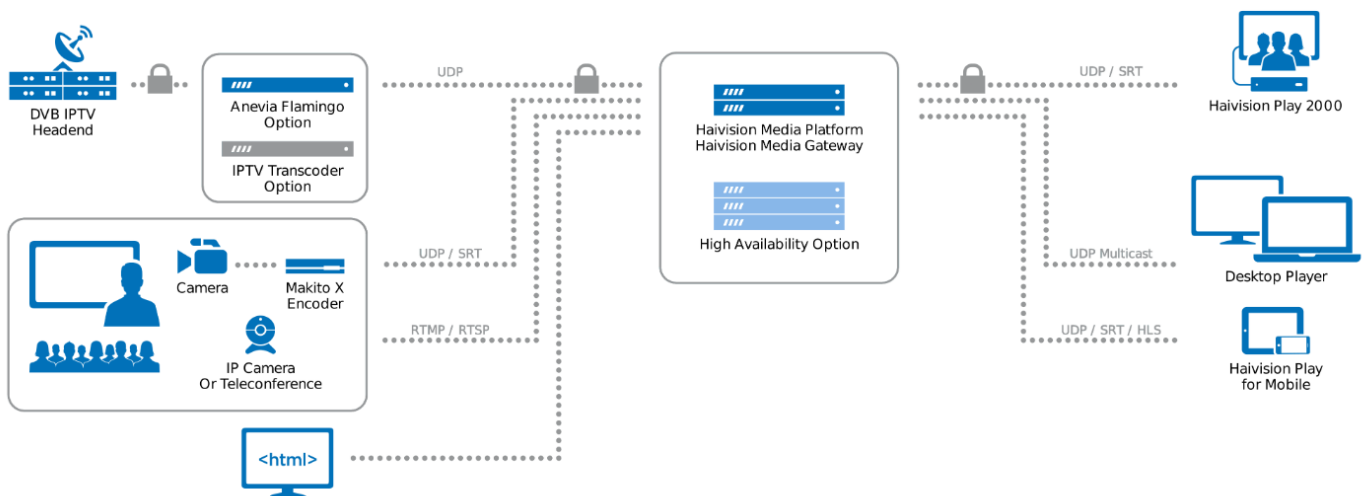
Haivision Media Platform is available in the following editions to suit different applications.

Enterprise Edition

Live All Hands, IPTV, Digital Signage

Haivision Media Platform Enterprise is a powerful multi-site live video distribution platform for streaming enterprise video content to employees watching inside and outside the corporate firewall, and for displaying IPTV content on TV screens throughout your organization.

The Haivision Media Platform Enterprise helps securely distribute live and on-demand broadcast-quality video, such as CEO all hands, company events, HR updates, product launches, and IPTV to employees watching on any screen globally - at headquarters, remote offices, and on the road.



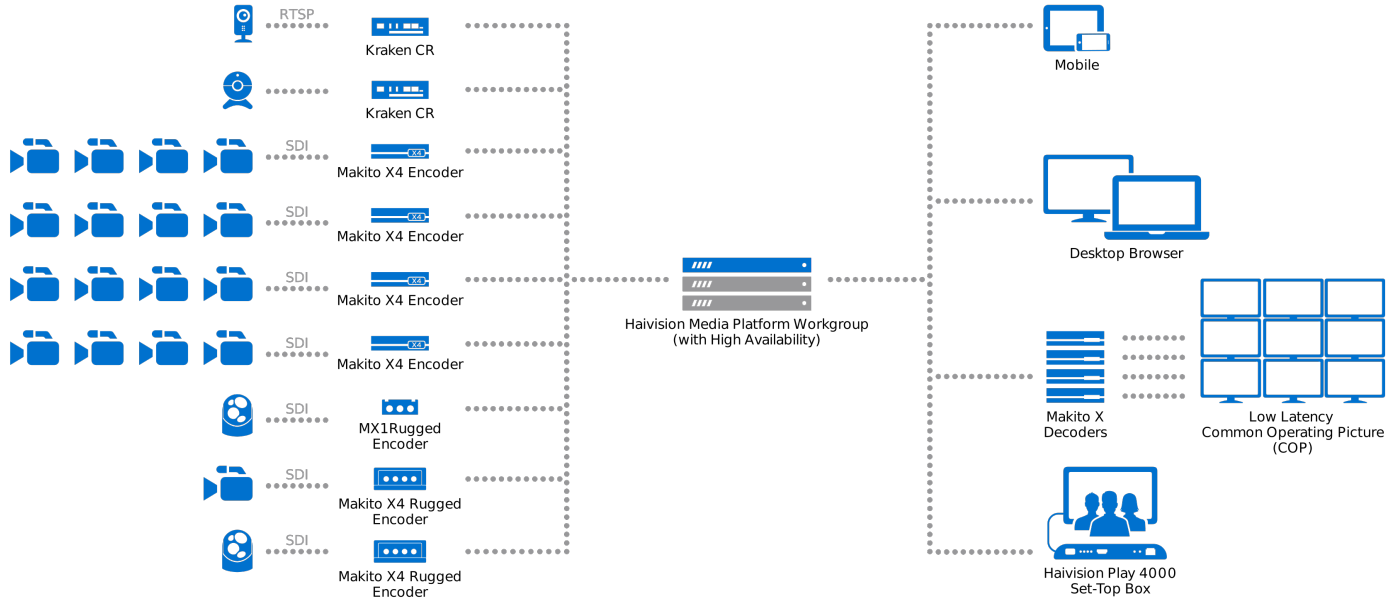
Note

The HMP Enterprise edition is expandable through licensing for: 2500 user/device license packs, 5 recording channel packs, High Availability (requires use of network storage), and eCDN (requires Haivision Media Gateway). For detailed information, please refer to Haivision's website at: <https://www.haivision.com>.

Workgroup Edition

High-capacity Live Video Recording & Low Latency Viewing Platform

Haivision Media Platform Workgroup is a powerful enterprise-grade video recording and streaming platform. With low-latency, multi-view playback and secure multi-site live video distribution, Haivision Media Platform Workgroup enables aggregation of high-quality, full-motion video (FMV) from the field for command and control, situational awareness, and after action reporting.



Note

The HMP Workgroup edition is expandable through license for: 2,500 user/device license packs, 5 recording channel packs, High Availability (requires use of network storage), IPTV & Channel Guide, Video-on-demand portal/content library, and eCDN (requires Haivision Media Gateway). For detailed information, please refer to Haivision’s website at: <https://www.haivision.com>.

Product Features

Key Haivision Media Platform features for each edition include the following:

Enterprise Workgroup

Live Internal Webcasts

Broadcast live all hands and town hall meetings so that employees can watch anywhere, on any device.

IPTV Streaming

Deliver broadcast TV channels along with live internal content to every screen throughout the organization.

Multisite eCDN

Distribute live streams and on-demand video across multiple enterprise locations via WAN and internet without overwhelming the network.

Unparalleled Security

Protect live and on-demand content from unauthorized viewing, copying, and redistribution with glass-toglass AES 128/256 encryption.

Permission-Based Authentication

Support for Active Directory, LDAP and SSO ensures that administrators can provide employees and set-top boxes with authorized content.

High Availability Option

Minimize the risk of system failure and maintain uptime through an optional secure inter-server database replication and status tracking system. See [High Availability Clustering Failover Support](#) for more details.

Multicast/Unicast

Support for virtually any WAN/LAN infrastructure with minimal IT intervention, including standards-based support for both unicast and multicast.

Set-Top Box Management

Centrally control and schedule when and where video is displayed on any STB-connected screen—in public areas, conference rooms, and auditoriums for group viewing.

High Quality Player

Ensure broadcast-quality viewing experiences with support for American closed captioning and user-selected languages on any HMP-supported device.

Remote Contribution with SRT

Haivision video encoding and SRT video transport technologies enable live video to be captured and delivered with low latency from anywhere.

Enterprise [Workgroup](#)

High-Capacity Video Recording

Record up to 50 high-quality video source simultaneously to enterprise-grade storage

Multi-View Live Streaming Playback

Live multi-view playback capabilities support up to 4 simultaneous streams in a desktop browser or more in a low-latency common operating picture (COP) video wall.

Low Latency Delivery

Seeing live events as close to real-time as possible is critical. HMP Workgroup delivers low latency video to the browser, ensuring that your team are able to respond to unfolding events as quickly as possible.

Multisite Distribution

Distribute live streams and on-demand video across multiple enterprise locations via WAN or Internet without overwhelming network capacity.

Trimming and Clipping

Simple-to-use editing tools make it easy to select portions of a longer video and trim them down to short clips for focused sharing of key events for After Action Reporting.

Hotmarking and Tagging

Mark key moments in real-time to facilitate enhanced Situational Awareness and efficient After Action Reporting.

High Availability

HMP Workgroup can maintain uptime through a secure inter-server database replication and status tracking system to minimize the risk of system failure. See [High Availability Clustering Failover Support](#) for more details.

Live Review Playback

Pause live streams, scrub back in time to review or tag critical events, then resume live playback without interrupting recording

Enterprise Integration and Security

Protect live and on-demand content from unauthorized viewing, copying, and redistribution with AES 128/256 encryption, adherence to industry best security frameworks, support for user authentication tools, and enterprise-grade shared storage.

Glass-to-Glass Solution

From encoders and transcoders, through Haivision Media Platform Workgroup, and all the way to playback on desktop, set-top-box and mobile devices, Haivision provides an entire secure solution.

Enterprise Integration and Security

Protect live and on-demand content from unauthorized viewing, copying, and redistribution with AES 128/256 encryption, adherence to STIG/NIST frameworks, and support for enterprise user authentication tools, all while leveraging enterprise-grade shared storage.

Multicast Support via Haivision Helper and Multicast Agent

⚠ Important

To configure browser-based multicast using Media Gateway, the Haivision Helper application must be installed on each user's computer (either by single/manual install or mass-deployment via an .MSI package). Haivision Helper is a cross-platform (Windows and OSX) utility that launches a multicast agent to enable multicast support.

The Haivision Helper application is available from the [Haivision Support Portal](#).

With Multicast Support on systems running the Haivision Helper application, HMP delivers a multicast agent to the user who receives a multicast Transport Stream and delivers a Web standard stream to the user's local Web browser. This helps reduce overbandwidth consumption on multicast enabled LANs.

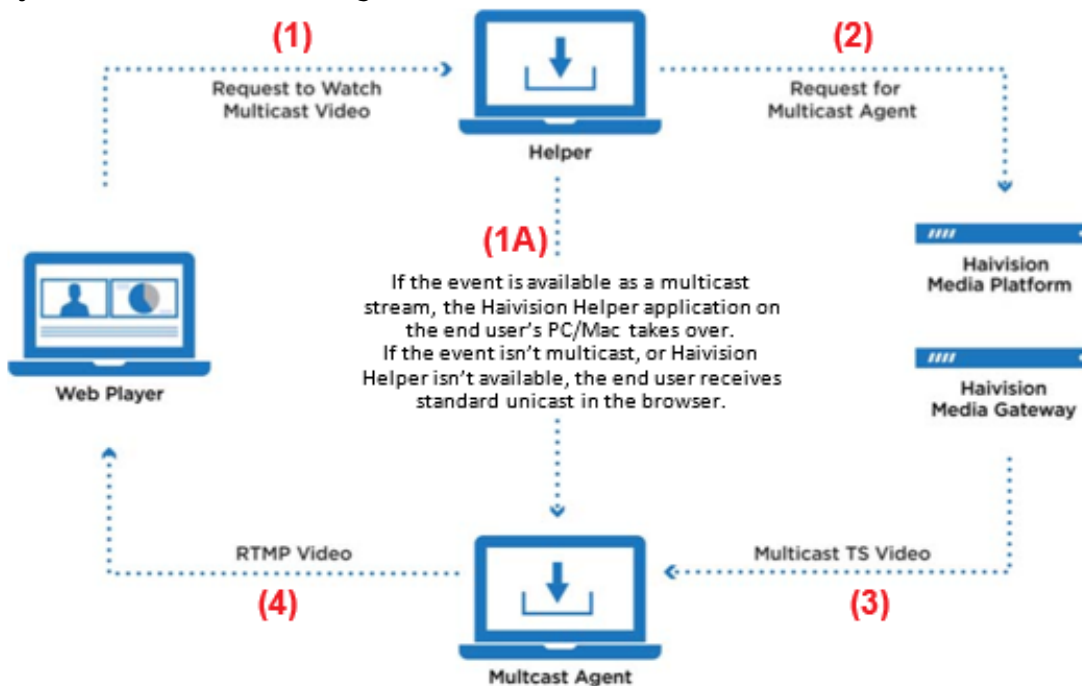
Following is a description of the process by which the Helper launches the multicast agent and enables multicast support:

1. **Request to Watch Multicast Video:** The end user clicks a link to a live video asset in their browser (on the HMP Portal or embedded player).

⚠ Note

The remaining steps are invisible to users.

2. If the event is available as a multicast stream, Haivision Helper on the end user's PC/Mac takes over. If the event is not multicast, or Haivision Helper is not available, the end user receives standard unicast in the browser.
3. **Request for Multicast Agent:** On HMP, Haivision Helper executes the multicast agent. If this is the user's first multicast request, Haivision Helper "fetches" the multicast agent from the nearest Media Gateway or HMP. The multicast agent is then held in cache for future use.



4. **Multicast TS Video:** The multicast agent joins the Multicast Group, and negotiates access and encryption for the video.

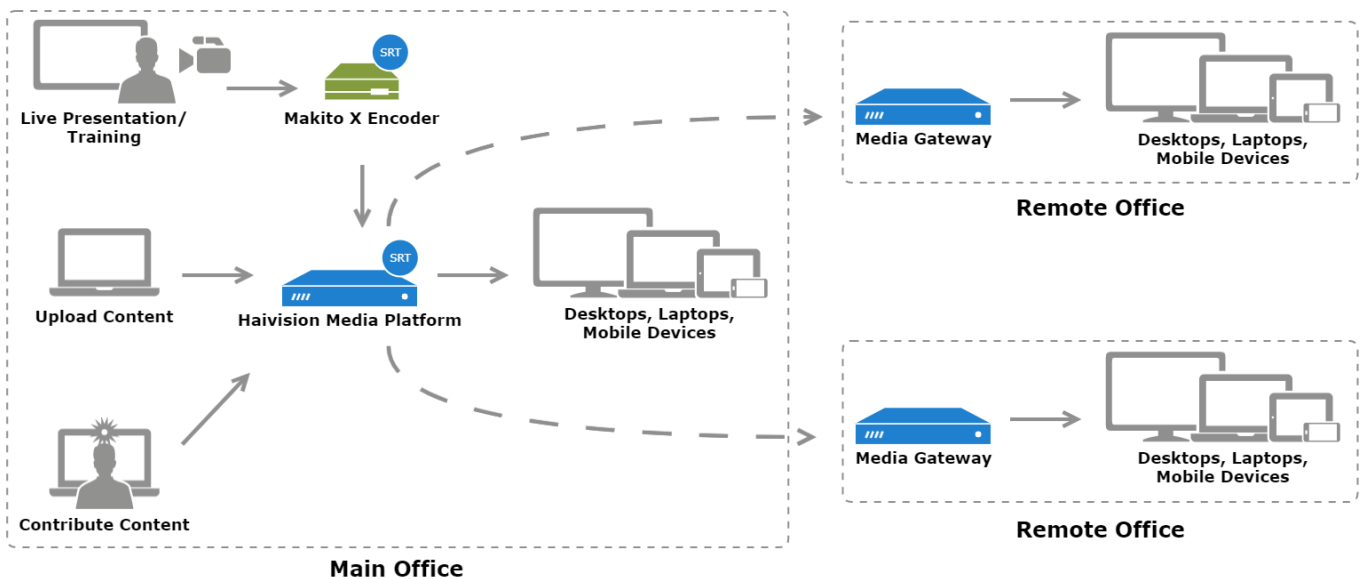
5. **RTMP Video:** The multicast agent converts the stream from Multicast TS to Native Web Video (RTMP is used for low latency), and the RTMP stream is delivered securely to the local browser over local host (all within the user's PC/Mac).

Note

For the latest information, please refer to the [Haivision Helper Documentation](#).

HMP-Media Gateway Pairing

A Haivision Media Platform server may be integrated with multiple Haivision Media Gateways in order to distribute video to remote locations. The Media Gateways provide a network of caching for HMP live and on-demand videos, allowing users at each location to watch video from their local gateway. For more information on pairing your HMP server with Media Gateways see [Pairing Media Gateways to HMP](#), and for more information on multi-site live distribution see [Configuring Multi-Site Live Distribution](#).



Related Topics

- [Pairing Media Gateways to HMP](#)

SRT (Secure Reliable Transport)

Haivision Media Platform supports Haivision's Secure Reliable Transport (SRT) from a Makito X encoder or Media Gateway as an input type. This enables end-to-end security and stream resiliency for recording and streaming applications. For more information, please refer to the [SRT Deployment Guide](#).

SRT is a transport technology that optimizes streaming performance across unpredictable networks, including the public Internet, for secure, reliable, low latency HD video. SRT as a protocol is included with Makito X encoders and decoders and Haivision's Media Gateway. HMP sources can be set up using either UDP or SRT protocol.

Related Topics

- [Configuring Secure Reliable Transport \(SRT\) Sources](#)

High Availability Clustering Failover Support

Important

All HMP HA clusters must be implemented by Haivision Field Services.

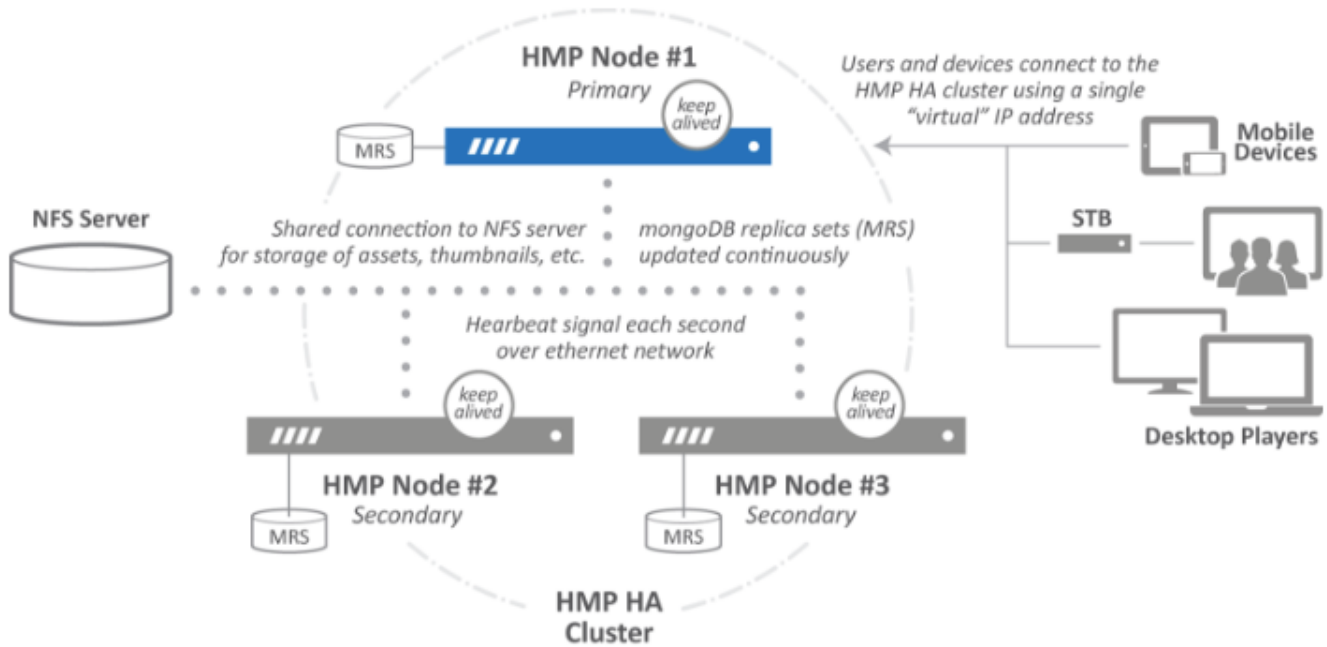
High Availability (HA) clustering provides a fault-tolerant HMP streaming solution. This licensed service is based on a cluster of three identically-provisioned servers (one primary and two secondary), plus one NFS server to serve as a media repository (not provided by Haivision).

The primary server provides all services while the secondary servers maintain a state of active readiness (online, but not providing services). This redundancy ensures that if the primary server fails for any reason, one of the secondary servers seamlessly assumes all services with minimal interruption.

Note

The HA feature *does not* guarantee fully uninterrupted service. In the event of a critical primary server failure, there is a momentary service interruption followed by automatic recovery. This failover takes a few seconds during which *some* interruption is unavoidable.

All three servers maintain a local copy of the HMP database, which stores all necessary data for operations. The secondary servers are continuously synced to ensure readiness to take over the primary role if needed.



For more information, see the [Haivision Support Portal](#).

Related Topics

- [Viewing High Availability Cluster Status](#)

Getting Started

This section describes how to access the Haivision Media Platform (HMP) Web interface and introduces basic administration and management functionality.

Important

Before proceeding, ensure that the appliance is set up correctly and all necessary network and A/V connections are established.

- For information on installing and connecting to a physical server, please refer to the [Server Quick Start Guide](#).
- To install an HMP virtual machine, refer to the [VMware Quick Start Guide](#).
- For the default sign-in credentials, refer to the *Important Notice* (postcard shipped with the unit or available from the Download Center on the [Haivision Support Portal](#)).

Topics Discussed

- [Accessing the HMP Web Interface](#)
 - [SSL Encryption](#)
- [Changing the Default Password](#)
- [Navigating the Interface](#)
- [Modifying the IP Address](#)
- [Creating a New Admin User](#)
- [Adding a Source](#)

Accessing the HMP Web Interface

Note

Newly installed systems default to the HTML5 "Modern" player. However, your system administrator may have set desktop browser playback to the "Legacy" Flash-based player. Therefore, your browser may need to be Flash-enabled to watch streams on the HMP web interface. Since Adobe Flash is no longer supported in the latest browser versions, streams may not be viewable. Contact your system administrator for more details.

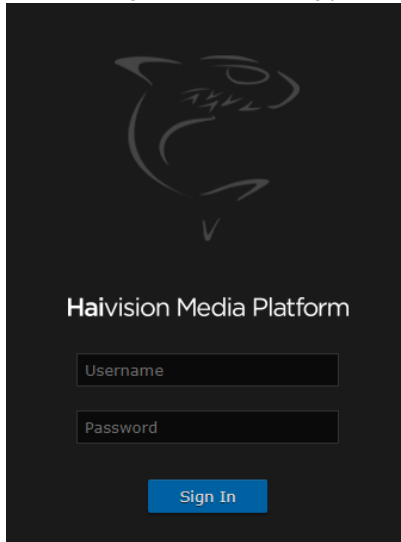
To access the Haivision Media Platform Web interface:

1. Open a Web browser of your choice, such as Chrome, Firefox, Safari, or Microsoft Edge (Internet Explorer no longer supported).
2. Type the URL or IP address for HMP in the browser's address bar and press **Enter**.

Note

When the browser accesses the HMP website, it requests the security certificate to confirm that the site is trusted. If a security certificate is not available or is self-signed, a Security Certificate warning appears. In this case, refer to [SSL Encryption](#) for details on how to supply HMP with an SSL security certificate to continue to the Sign-in screen.

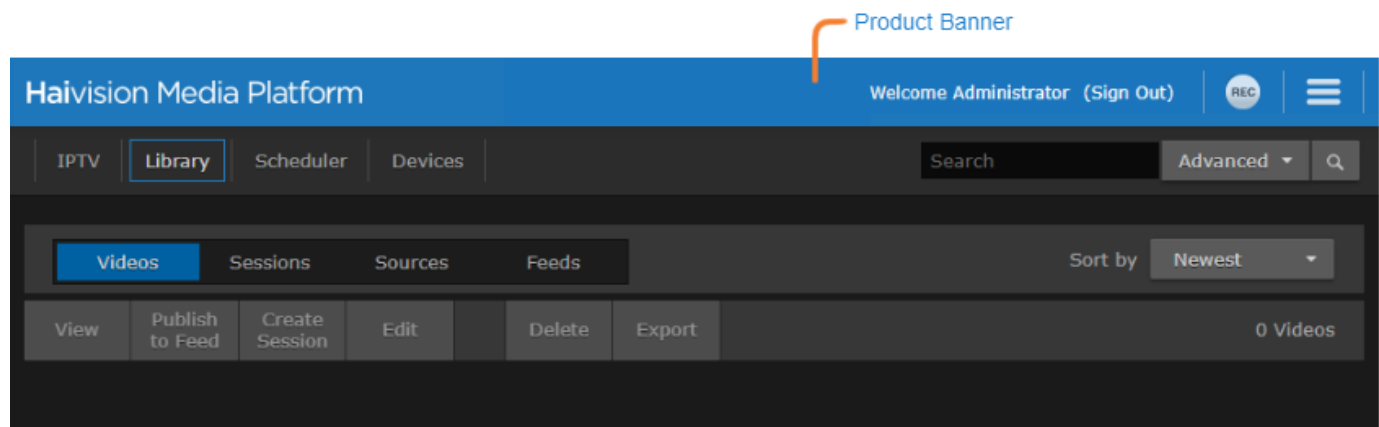
- On the Sign-in screen, type the Username and Password and click **Sign In**.



Note

For the default sign-in credentials, refer to the *Important Notice* (postcard shipped with the unit or available from the Download Center on the [Haivision Support Portal](#)).

After you have successfully signed in, the Web interface opens with your account information displayed in the product banner.



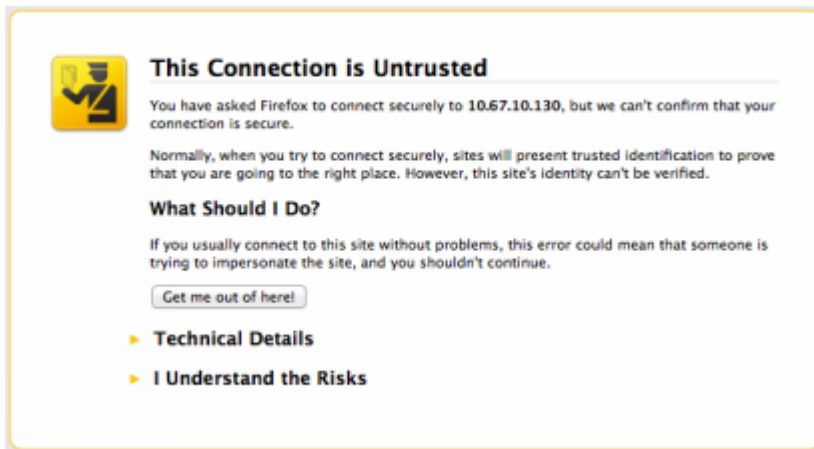
Related Topics

- [Creating a New Admin User](#)

SSL Encryption

Haivision Media Platform is encrypted to provide secure interactions with your devices. When you sign into the HMP interface, you are automatically redirected to the HTTPS site using port 443. As a result, the browser requests the security certificate to confirm that the site is trusted.

HMP ships with a self-signed Secure Sockets Layer (SSL) certificate key set which works with any configured server hostname. However, web browsers do not consider self-signed certificates to be trusted, because they are not signed by a Certificate Authority. Consequently, when accessing the website with a self-signed certificate, users see a security warning and are prompted for authorization as shown below.



Supplying HMP with an SSL security certificate eliminates the security warning, provides a means for users to verify a website, and ensures that the connection is secure. See [Managing Certificates](#) for more details.

Changing the Default Password

⚠ Caution

For security purposes, Haivision strongly advises you to change the default passwords during initial configuration.

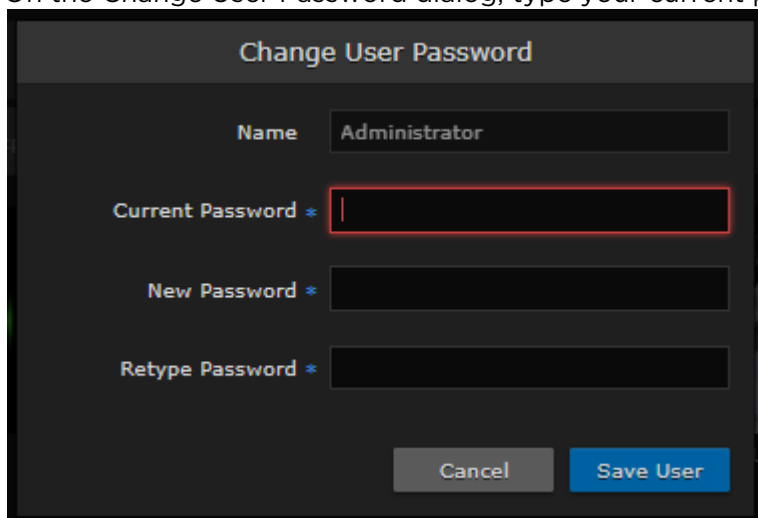
⚠ Note

`haiadmin` is a special system user intended primarily for initial setup and system troubleshooting. It is not intended for regular use because it has unrestricted access privileges that cannot be changed. For day-to-day system control and administration, we strongly advise you to create a regular administrative user with a secure password. See [Creating a New Admin User](#).

To change the password for the current user:

1. Click the user name (e.g., Administrator) on the toolbar.

2. On the Change User Password dialog, type your current password in the Current Password field.




3. Type the new password in the New Password field and again in the Retype Password field.
4. Click **Save User**.

The password change takes effect immediately.

Navigating the Interface

When you first sign in, the Haivision Media Platform web interface opens to the Library (showing the Videos list).

- If you activate the Portal, the interface opens to the Portal. The Portal is an optional feature that your organization can use to create a custom landing (home) page for users. For more information, please refer to [Configuring Feeds and Activating the Portal](#).
- Depending on your license, an IPTV, Live Review, and/or Layouts link also appears on the navigation bar.
- To open the Portal, view live IPTV content, manage layouts, schedule an event, or manage devices (set-top boxes), click the option on the navigation bar. Clicking an option opens the selected screen.
- Clicking the  icon opens the navigation drop-down menu, which contains the following items:
 - **Administration** — Opens the administration screen.
 - **Import/Export** — Allows you to import or export videos. See [Managing Imports and Exports](#) in the User's Guide.
 - **Keyboard Shortcuts** — Lists shortcuts available for the current screen you are viewing.
 - **User Preferences** — Allows you to adjust the UI brightness and contrast, and reset the HMP stored preferences.
 - **About** — Lists the current HMP version number.
 - **What's New** — Displays a list of new HMP features.
 - **Help** — Opens the Haivision InfoCenter. If you do not have a connection to the Internet, opens a bundled HTML version of the HMP documentation.

For details on using the non-administrator functions of the HMP interface, including viewing and search options, see the [User's Guide](#).

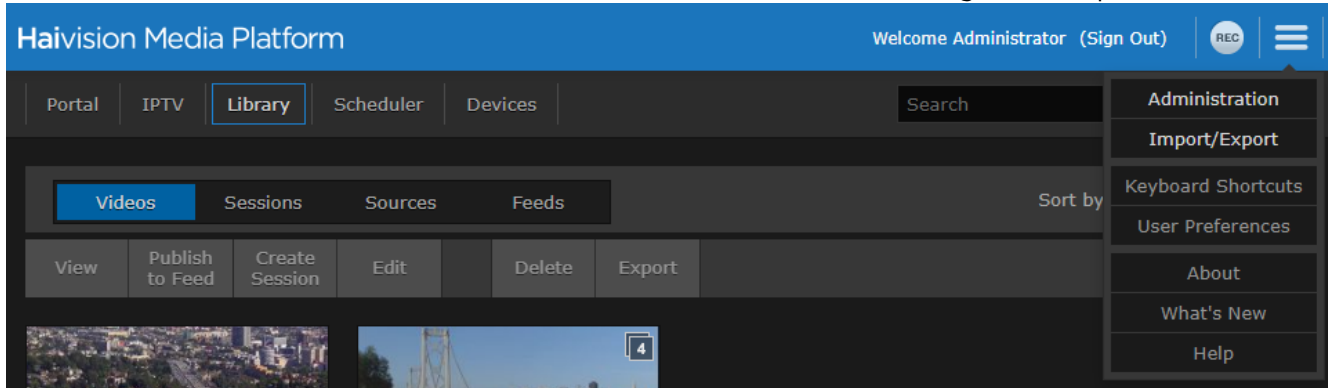
Modifying the IP Address

Follow these steps to change the IP address or other network settings from the Web Interface.

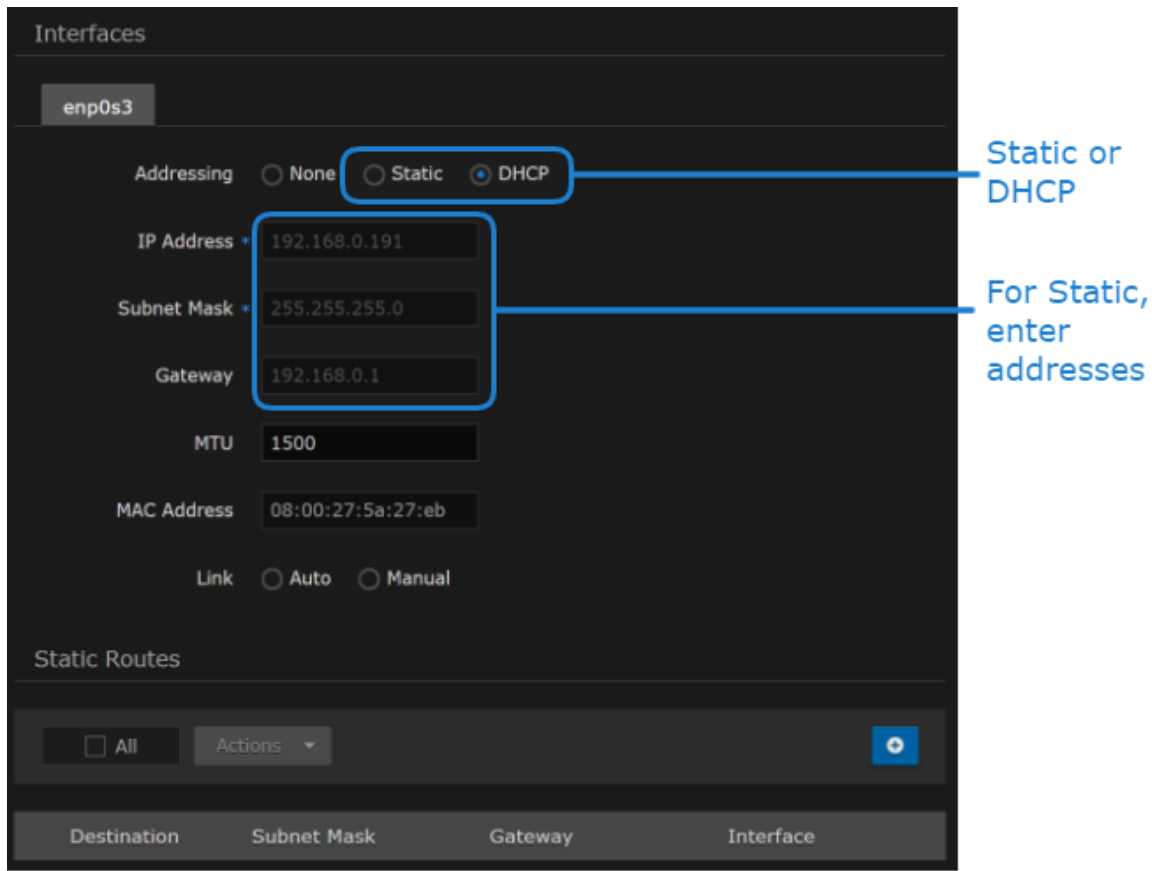
Tip

You can also modify network settings by connecting directly to the Console UI. To do so, connect a keyboard and monitor to the server (refer to the [Server Quick Start Guide](#)). You can also access the Console UI remotely using a secure shell (SSH) connection. For more information, see [Using the Console UI with Haivision Hardware](#).

1. Click the  icon on the banner and select **Administration** from the navigation drop-down menu.



2. On the Administration page, click **System Settings** on the toolbar and then click **Network** on the sidebar.
3. On the Network Configuration page, for the first network interface (enp0s3 in the following example), either:
 - Select DHCP to automatically assign an IP address from a DHCP server, or
 - Select Static and enter a valid IP address, subnet mask, and gateway to work in your environment.





4. Click **Save Settings**, and then click **Reboot** and **Confirm** for the changes to take effect.
5. After the system reboots, sign in again using the new IP address, if applicable, to continue.

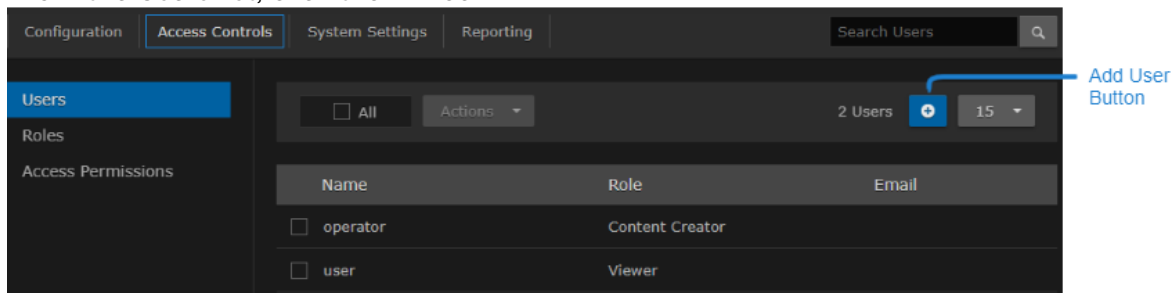
Related Topics

- [Configuring Network Settings](#)

Creating a New Admin User

To create a new administrative user from the web interface:

1. Click the  icon on the toolbar and select **Administration** from the navigation drop-down menu.
2. Click **Access Controls** on the toolbar and then click **Users** on the sidebar.
3. From the Users list, click the  icon.



- On the Add User dialog, enter the display name, username/password for logging in, and Email address to associate with the user account.

The screenshot shows a dark-themed 'Add User' dialog box. It has the following fields: 'Name' (with a red border), 'Username', 'Password', 'Retype Password', 'Email', and 'Role' (a dropdown menu currently showing 'None'). At the bottom, there are two buttons: 'Cancel' and 'Add User'.

- For the Role, select Administrator.

Tip

Haivision Media Platform uses roles with pre-defined permissions to provide users or groups with controlled access to sessions and recordings. Users must be assigned a role to sign in. Users may also be assigned access permissions for content rights (recordings and sessions) by administrators or other users.

- Click **Add User**.
The new user is added to the Users list.
- Click **Sign Out** on the navigation bar and then sign in with the new admin credentials to have full administrative permissions.

Note

For more information on managing users/groups and roles, as well as connecting Haivision Media Platform to a directory server, see [Managing Users](#).

Adding a Source

A source is an incoming unicast or multicast video stream or IPTV channel that can be recorded or viewed live. Haivision Media Platform provides access to video streams originating from Haivision Makito and Makito X encoders or other systems that produce compatible MPEG-TS video streams. When setting up HMP, you need to specify the streaming A/V sources to be available for content creators and others to view and capture.

To add a source:

- On the Administration page, click **Configuration** on the toolbar and then click **Sources** on the sidebar.
- From the Sources list, click the **+** icon.
- On the Add Source dialog, enter the Name, Description, IP Address, and Port for the source. Leave the default Receiver (HMP) and Type (UDP).
 - For a unicast stream, uncheck the Multicast Stream checkbox.

- To configure the source as an IPTV channel (available for viewing from a Haivision Play Set-Top Box), check the IPTV checkbox.
- To display EPG data on set-top boxes, toggle the EPG button to **On** and select the Schedule. (EPG must be licensed on your system.)
- For the Haivision Play Set-Top Box, to use the source URL directly instead of an HLS version, check the View Direct checkbox.

4. Click **Add Source**.

The new source is added to the Sources list:

Name	IP Address	Type	Gateway
<input type="checkbox"/> New Source	0.0.0.0:1234	UDP	Mgt. Server

After a source is available, the system is ready for streaming, scheduling, and recording live events.

Note

Multicast playback is a licensed feature and must be purchased separately. Please contact Haivision for more information. Multicast playback requires at least one Haivision Media Gateway. Also the Haivision Helper application must be installed on each user’s computer. The Helper application is available from the Haivision Support Portal at: <https://support.haivision.com>. For more information, see the [Haivision Helper Documentation](#).

Related Topics

- [Configuring Feeds and Activating the Portal](#)
- [Managing Sources](#)

Configuring HMP

This section describes how to configure your Haivision Media Platform (HMP), including the Portal, sources, IPTV channels, locations, paired Media Gateways, and Set-top Box administration.


Topics Discussed

- [Adding Export Destinations](#)
- [Configuring Feeds and Activating the Portal](#)
- [Configuring IPTV Channels](#)
- [Configuring Locations](#)
- [Pairing Media Gateways to HMP](#)
- [Defining Metadata](#)
- [Setting Default Set-Top Box Values](#)
- [Managing Sources](#)
- [Managing Stream Outputs](#)
- [Re-Branding the User Interface](#)
- [Configuring Video and Session Settings](#)
- [Using an External Player to View Sessions](#)
- [Adjusting STB Player Tuning](#)

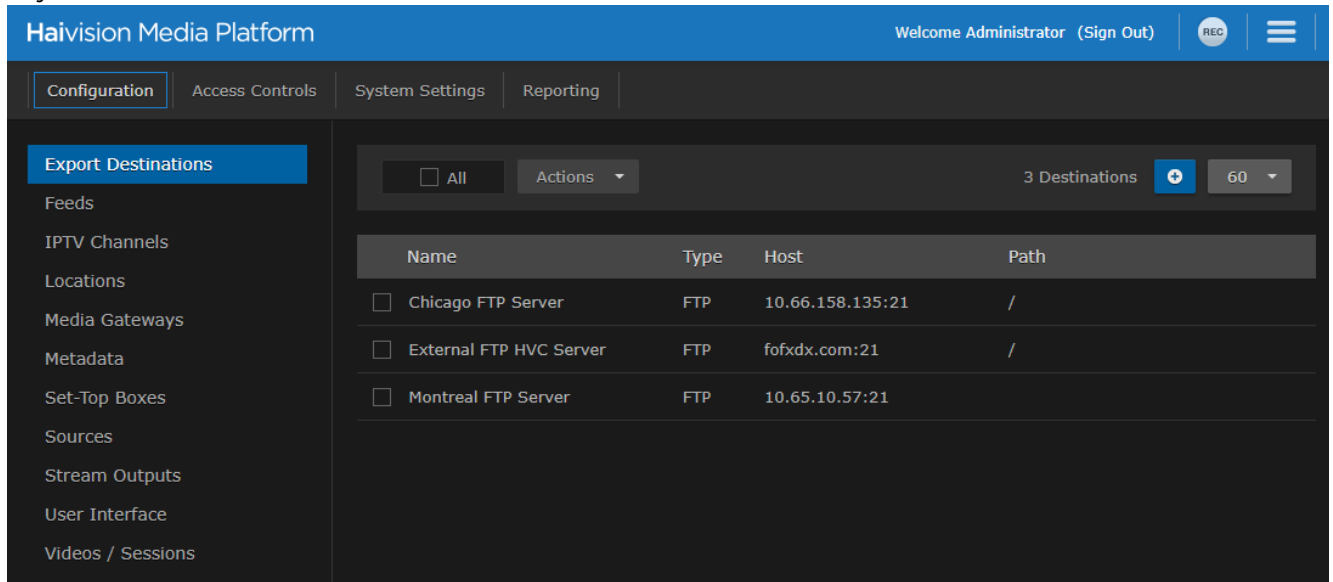
Adding Export Destinations

When setting up Haivision Media Platform, administrators can add export destinations for video and metadata to FTP/FTPS servers and the Haivision Video Cloud (HVC) platform. Then, these destinations are available for users to select when exporting videos. For more information, see [Managing Exports](#) and [Exporting Videos](#) in the User's Guide.

To view and manage the export destinations:

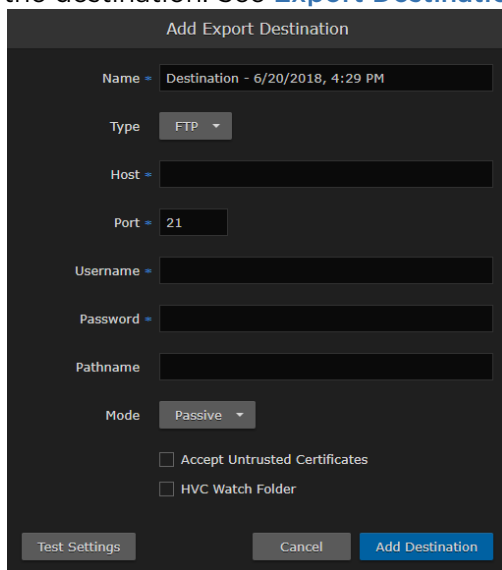
1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **Export Destinations** on the sidebar.
The Export Destinations pane opens, displaying the list of defined destinations for your platform, if

any.



To add an export destination:

1. From the Export Destinations pane, click the **+** icon.
2. On the Add Export Destination dialog, enter a destination name and enter/select values to define the destination. See [Export Destination Settings](#).




3. To test the connection, click **Test Settings**.
4. Click **Add Destination**. The new export destination is added to the list.

Related Topics

- [Export Destination Settings](#)

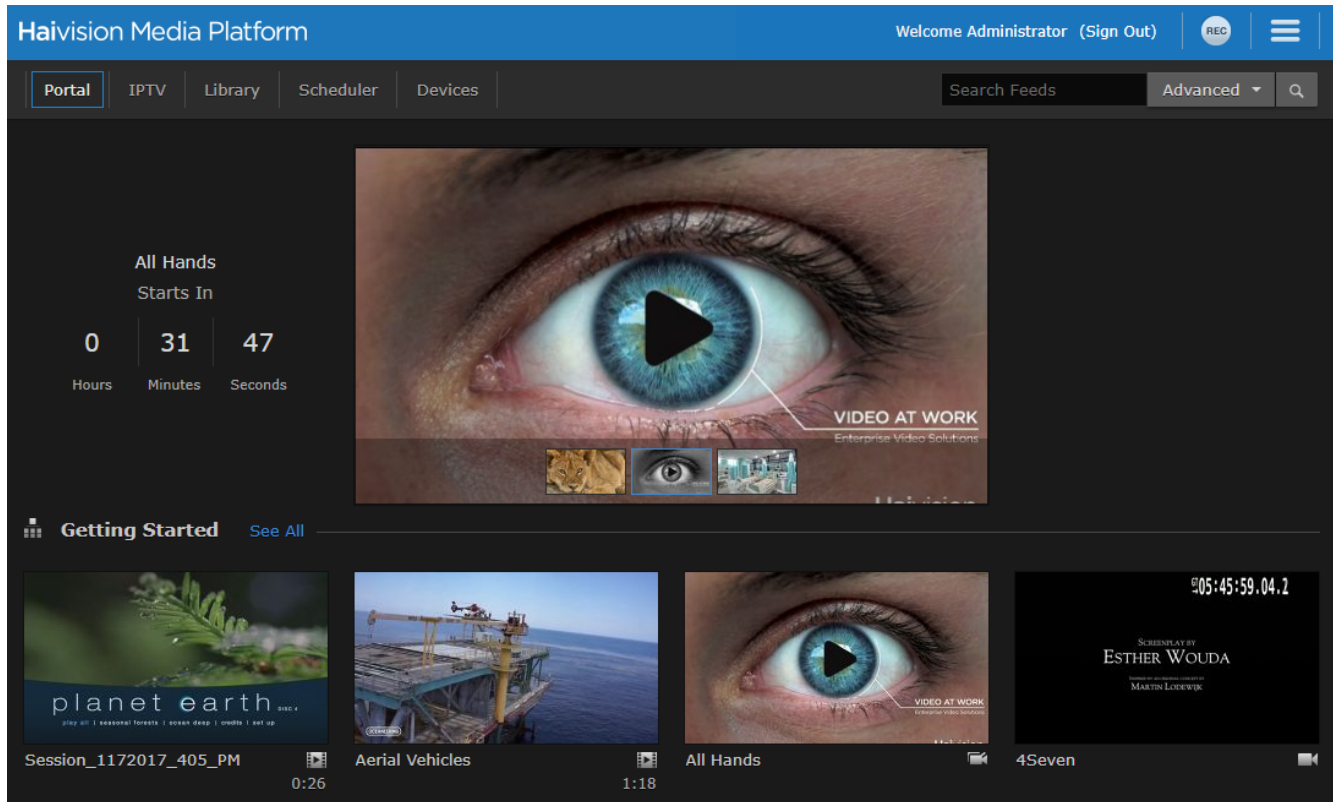
Export Destination Settings

The following table lists the Export Destination configuration settings:

Setting	Default	Description/Values
Name	—	Label for the destination.
Type	FTP	Select the protocol type: <ul style="list-style-type: none"> • FTP: File Transfer Protocol • FTPS: FTP with explicit Transport Layer Security (TLS)
Host	—	Destination server's DNS hostname or IP address.
Port	21	Port number for the destination server.
Username	—	Login username for the site.
Password	—	Username's password.
Pathname	—	(Optional) File path to use on the server, or leave blank for the server's default path.
Mode	Passive	Select the FTP data connection mode provided by your FTP administrator: <ul style="list-style-type: none"> • Passive: Passive mode may be used in situations where the client is behind a firewall and unable to accept incoming TCP connections. By default, most Web browsers use passive (PASV) mode, which more easily traverses end-user firewalls. • Active: In active mode, the client creates a TCP control connection.
Accept Untrusted Certificates	Disabled	Check this checkbox to allow Haivision Media Platform to connect to an FTPS server that is using an untrusted SSL certificate.
HVC Watch Folder	Disabled	Check this checkbox to create an HVC-compatible mRSS (Media RSS) metadata file. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>This file contains information about a recording (e.g. author, duration, key/value metadata) that can be ingested by platforms such as HVC. An HVC workflow automation script can be configured to use this watch folder on HMP.</p> </div>


Configuring Feeds and Activating the Portal

The Portal is an optional feature that Haivision Media Platform administrators can use to create and maintain a custom landing (home) page for your organization. The Portal displays thumbnails of selected videos, sessions, and sources – grouped by video feed. When enabled, the Portal is the first screen users see after they sign into HMP. Viewers can browse feeds, search for items, and launch the video, session, or source. For the Portal user workflow, see [Exploring the Web Interface](#) in the User’s Guide.



From the Administration’s Feeds pane, administrators can create, change access permissions, and manage Portal feeds, including turning the Portal on and off. After turning on the Portal, content managers can populate the feeds and promote items to “Suggested” and “Featured” using the Library’s Feeds editor. For details, see [Managing Feeds](#) in the User’s Guide.

To view and manage the Portal:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then **Feeds** on the sidebar. The Feeds pane opens, displaying the list of defined feeds, if any.
3. To activate the Portal, toggle the Portal Access button to **On**. The Portal option is added to the navigation bar when not on the Administration screen.
4. To allow Feed permissions to take precedence over the Access Permissions assigned to individual videos, sessions, or sources, toggle the Use Feed Permission button to **On**.

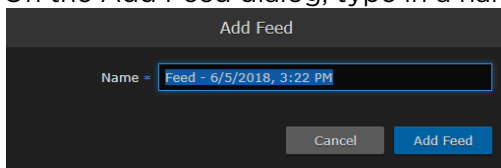
Note

By default, viewing permissions are enforced from the video asset itself, and users are prevented from watching content that they do not have access to. However, the **Use Feed Permission** toggle option allows administrators to reverse this. This setting saves content managers from having to change access permissions for all individual items in feeds. Instead, they simply edit the access permissions of the feed.

The next step is to begin adding feeds.

To add a video feed:

1. On the Feeds pane, click the **+** icon.
2. On the Add Feed dialog, type in a name for the feed.

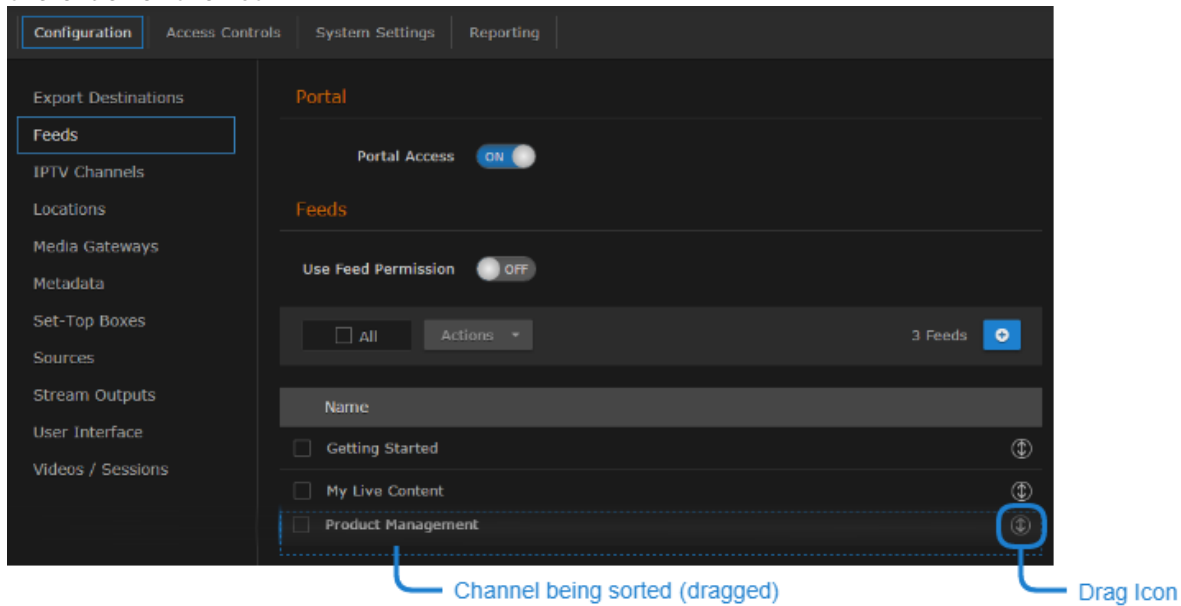


3. Click **Add Feed**.
The new feed is added to the Feeds list.
4. To change access permissions for a feed, click on the feed from the list, and on the Information pane, click the **Access** tab. Follow the steps in [Sharing Items](#) in the User's Guide.

Note

See the note in the previous section regarding Feed Permissions.

5. To change the feed display order, on the Feeds list, click the **↕** icon for a feed and drag it to adjust the order of the list.




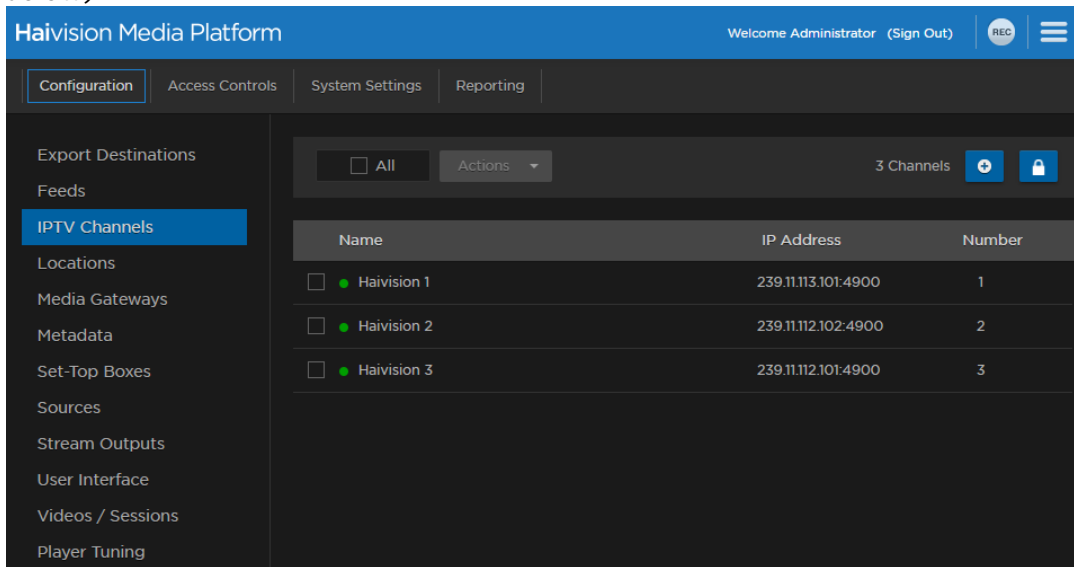
For details on populating the feeds using the Library's Feeds editor, see [Managing Feeds](#) in the User's Guide.

Configuring IPTV Channels


IPTV channels are sources that have been enabled for IPTV deployment for Haivision Play Set-Top Boxes. If your system is licensed for IPTV, you can setup IPTV channels and assign access from here or from the Sources pane.

To view and manage IPTV channels:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **IPTV Channels** on the sidebar. The IPTV Channels pane opens, displaying the list of defined channels for your platform (as shown below).



To add an IPTV channel:

1. From the IPTV Channels pane, click the  icon. This opens the Add Source dialog, with the IPTV Channel checkbox checked.
2. Enter the desired channel name, channel number, and add the various settings to define the source. See [Source Settings](#) for details.
3. Click the **Add Source** button.

The new source is added to both the IPTV Channels and Sources lists.

Changing IPTV Channel Numbers

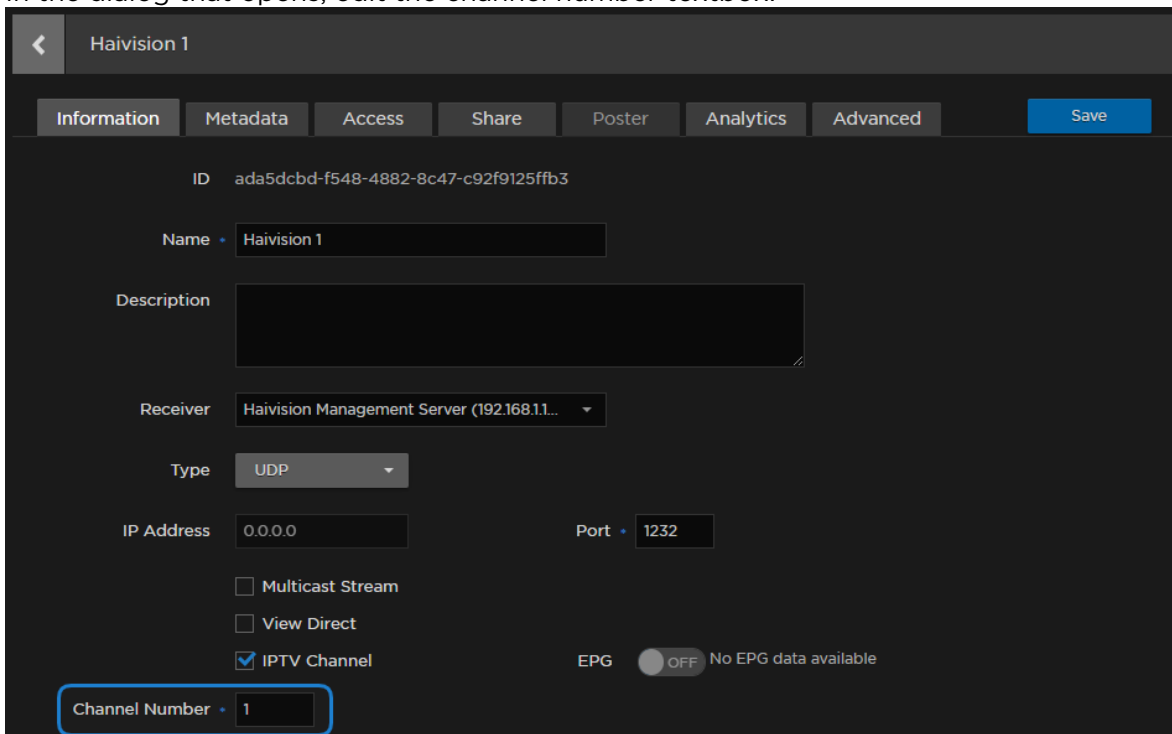
The number assigned to each IPTV channel can be changed by either:


- Editing each channel/source.
- Dragging-and-dropping the channels in the list.

Editing each Channel Dragging-and-Dropping each Channel

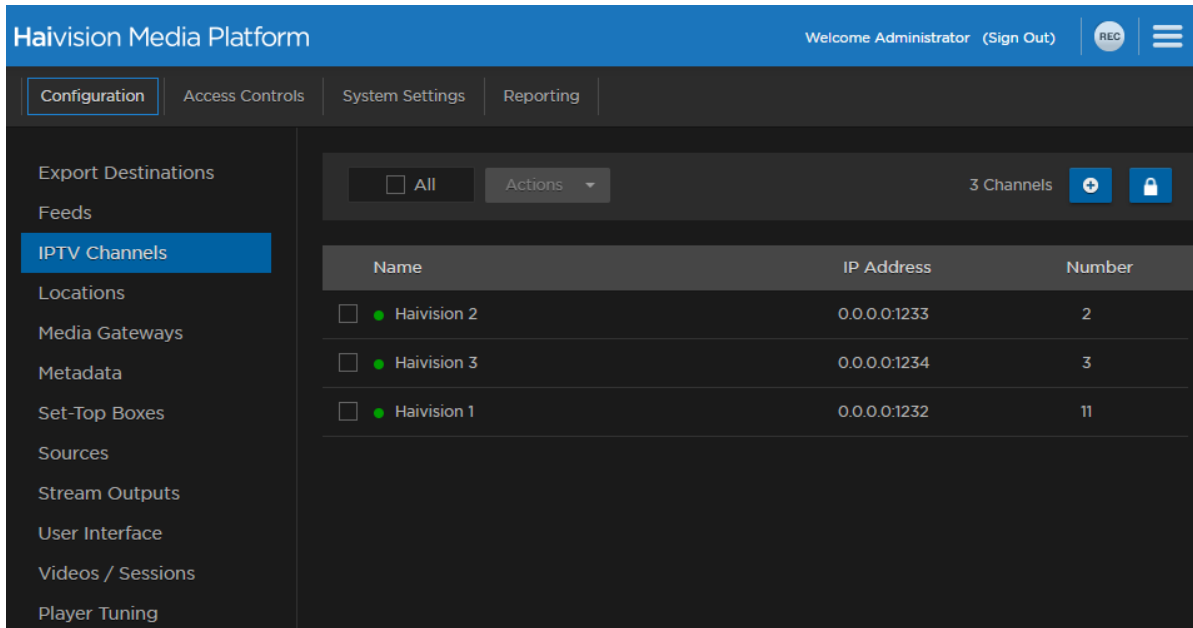
To change the channel numbers by editing the channels/sources:

1. Click the channel to edit.
2. In the dialog that opens, edit the channel number textbox:



3. Click the **Save** button.
4. Click the  button to return to the IPTV channel list.
5. Repeat steps 1-4 for each channel you wish to edit.

The channel list is updated with the new channel numbers and new channel order, if applicable.




Editing each Channel [Dragging-and-Dropping each Channel](#)

Important

Before using the drag-and-drop method, please note the following:

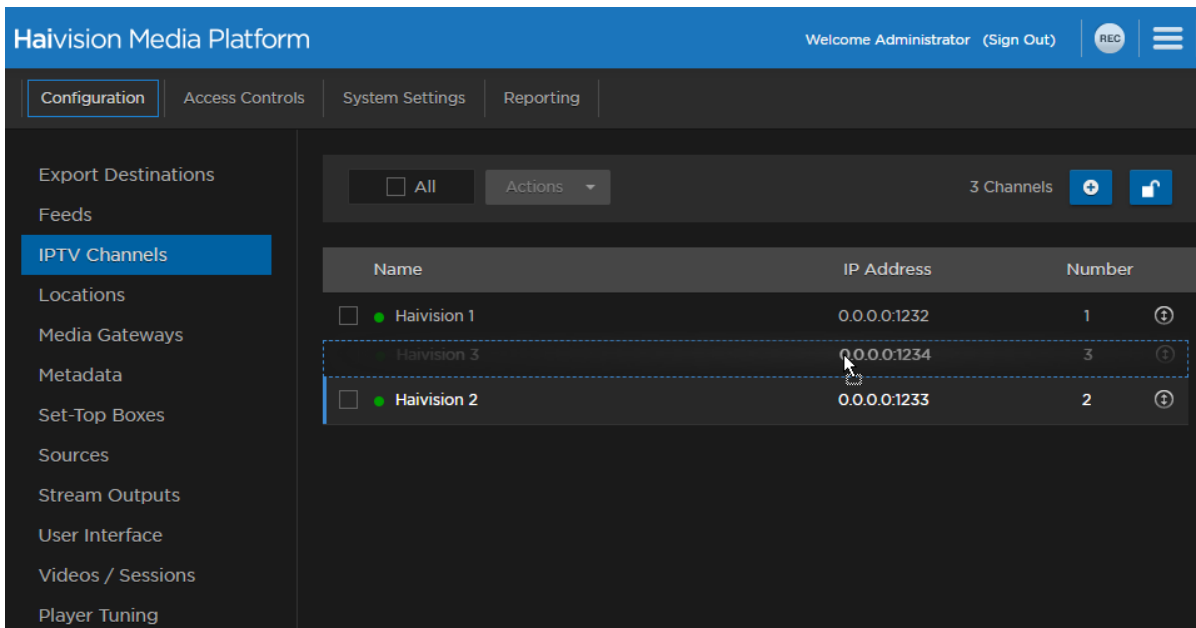
- You cannot undo a drag-and-drop operation.
- Updates to the channel list are automatically saved as they are made.
- Dragging-and-dropping one channel may update the channel numbers of others.

To drag-and-drop channels to change the channel numbers:

1. Click the  button to enable the drag-and-drop function.
2. Drag a channel you wish to change the channel number of to the new channel number location. In the below screenshot, channel #3 is dragged above channel #2.

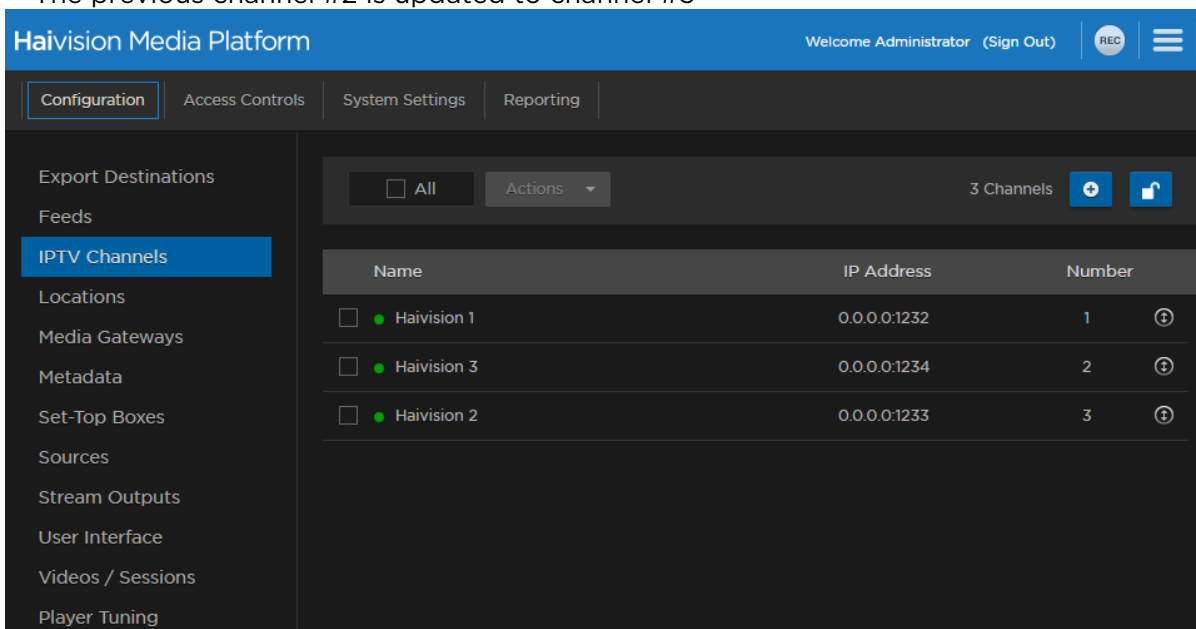
Tip

Press the **ESC** key on your keyboard to cancel the drag-and-drop operation.



Drop the channel in the new desired place in the channel list.

3. The channel number for the channel you dragged-and-dropped is updated, and if necessary all channels that follow it. For example, in the following screenshot, after dropping channel #3 above channel #2:
 - The previous channel #3 is updated to channel #2
 - The previous channel #2 is updated to channel #3



4. Click the  button to disable the drag-and-drop function.

Example IPTV Drag-and-Drop Operations

Given the following channel list, see the following tabs for various outcomes using the drag-and-drop function.

All		Actions	8 Channels		
Name	IP Address	Number			
<input type="checkbox"/> ● Haivision 1	0.0.0.0:1232	1			
<input type="checkbox"/> ● Haivision 2	0.0.0.0:1233	2			
<input type="checkbox"/> ● Haivision 3	0.0.0.0:1234	3			
<input type="checkbox"/> ● Haivision 10	0.0.0.0:1235	10			
<input type="checkbox"/> ● Haivision 11	0.0.0.0:1236	11			
<input type="checkbox"/> ● Haivision 12	0.0.0.0:1237	12			
<input type="checkbox"/> ● Haivision 20	0.0.0.0:1238	20			
<input type="checkbox"/> ● Haivision 30	0.0.0.0:1239	30			

[Drag #10 to Top](#) Drag #11 before #10 Drag #10 after #20 Drag #30 after #11

After dragging channel #10 to the top of the list:

All		Actions	8 Channels		
Name	IP Address	Number			
<input type="checkbox"/> ● Haivision 10	0.0.0.0:1235	10			
<input type="checkbox"/> ● Haivision 1	0.0.0.0:1232	1			
<input type="checkbox"/> ● Haivision 2	0.0.0.0:1233	2			
<input type="checkbox"/> ● Haivision 3	0.0.0.0:1234	3			
<input type="checkbox"/> ● Haivision 11	0.0.0.0:1236	11			
<input type="checkbox"/> ● Haivision 12	0.0.0.0:1237	12			
<input type="checkbox"/> ● Haivision 20	0.0.0.0:1238	20			
<input type="checkbox"/> ● Haivision 30	0.0.0.0:1239	30			

Channel #10 becomes channel #1. The previous channels #1-3 are renumbered to #2-4.

Name	IP Address	Number
<input type="checkbox"/> Haivision 10	0.0.0.0:1235	1
<input type="checkbox"/> Haivision 1	0.0.0.0:1232	2
<input type="checkbox"/> Haivision 2	0.0.0.0:1233	3
<input type="checkbox"/> Haivision 3	0.0.0.0:1234	4
<input type="checkbox"/> Haivision 11	0.0.0.0:1236	11
<input type="checkbox"/> Haivision 12	0.0.0.0:1237	12
<input type="checkbox"/> Haivision 20	0.0.0.0:1238	20
<input type="checkbox"/> Haivision 30	0.0.0.0:1239	30

Drag #10 to Top Drag #11 before #10 Drag #10 after #20 Drag #30 after #11

After dragging channel #11 to between channel #3 and #10:

Name	IP Address	Number
<input type="checkbox"/> Haivision 1	0.0.0.0:1232	1
<input type="checkbox"/> Haivision 2	0.0.0.0:1233	2
<input type="checkbox"/> Haivision 3	0.0.0.0:1234	3
<input type="checkbox"/> Haivision 11	0.0.0.0:1236	11
<input type="checkbox"/> Haivision 10	0.0.0.0:1235	10
<input type="checkbox"/> Haivision 12	0.0.0.0:1237	12
<input type="checkbox"/> Haivision 20	0.0.0.0:1238	20
<input type="checkbox"/> Haivision 30	0.0.0.0:1239	30

Channel #11 becomes channel #4. No other channel numbers are changed.

Name	IP Address	Number
Haivision 1	0.0.0.1232	1
Haivision 2	0.0.0.1233	2
Haivision 3	0.0.0.1234	3
Haivision 11	0.0.0.1236	4
Haivision 10	0.0.0.1235	10
Haivision 12	0.0.0.1237	12
Haivision 20	0.0.0.1238	20
Haivision 30	0.0.0.1239	30

Drag #10 to Top Drag #11 before #10 Drag #10 after #20 Drag #30 after #11

After dragging channel #10 to between channel #20 and #30:

Name	IP Address	Number
Haivision 1	0.0.0.1232	1
Haivision 2	0.0.0.1233	2
Haivision 3	0.0.0.1234	3
Haivision 11	0.0.0.1236	11
Haivision 12	0.0.0.1237	12
Haivision 20	0.0.0.1238	20
Haivision 10	0.0.0.1235	10
Haivision 30	0.0.0.1239	30

Channel #10 becomes channel #21. No other channel numbers are changed.

Name	IP Address	Number
Haivision 1	0.0.0.0:1232	1
Haivision 2	0.0.0.0:1233	2
Haivision 3	0.0.0.0:1234	3
Haivision 11	0.0.0.0:1236	11
Haivision 12	0.0.0.0:1237	12
Haivision 20	0.0.0.0:1238	20
Haivision 10	0.0.0.0:1235	21
Haivision 30	0.0.0.0:1239	30

Drag #10 to Top Drag #11 before #10 Drag #10 after #20 Drag #30 after #11

After dragging channel #30 to between channel #11 and #12:

Name	IP Address	Number
Haivision 1	0.0.0.0:1232	1
Haivision 2	0.0.0.0:1233	2
Haivision 3	0.0.0.0:1234	3
Haivision 10	0.0.0.0:1235	10
Haivision 11	0.0.0.0:1236	11
Haivision 30	0.0.0.0:1239	30
Haivision 12	0.0.0.0:1237	12
Haivision 20	0.0.0.0:1238	20

Channel #30 becomes channel #12 and channel #12 is renumbered to #13.

Name	IP Address	Number
<input type="checkbox"/> Haivision 1	0.0.0.0:1232	1
<input type="checkbox"/> Haivision 2	0.0.0.0:1233	2
<input type="checkbox"/> Haivision 3	0.0.0.0:1234	3
<input type="checkbox"/> Haivision 10	0.0.0.0:1235	10
<input type="checkbox"/> Haivision 11	0.0.0.0:1236	11
<input type="checkbox"/> Haivision 30	0.0.0.0:1239	12
<input type="checkbox"/> Haivision 12	0.0.0.0:1237	13
<input type="checkbox"/> Haivision 20	0.0.0.0:1238	20

Configuring Locations

When setting up Haivision Media Platform, administrators can define additional site locations (for example, satellite offices). The purpose is to define networks on which users reside to route users through the closest location and to limit the distribution of videos based on a user’s location. Locations are typically used to set up HMP-Media Gateway pairings. The goal is to set up locations to “push” video as close as possible to users (at remote locations), using standard network definitions to identify the user location and the closest streaming device (i.e., Media Gateway) location.

For multi-site live distribution, select the gateways that will deliver video to the location. Each location can have up to 15 gateways.

Note

- You must be licensed for Multi-site eCDN to add more than one location.
- For more information on HMP-Media Gateway pairing, see [Pairing Media Gateways to HMP](#).
- All Media Gateways within the same HMP location must be configured with valid certificates to prevent unpredictable viewing behaviors with HLS streams.

Multicast Playback

If licensed on your system, HMP delivers multicast outputs from Media Gateways directly to browsers running on users’ desktops (PC/Mac) when the network supports multicast (MPEG2-TS). To set up multicast support, simply configure each HMP location with one or more ranges of multicast addresses. HMP then provides these addresses to the location’s Media Gateway to use for multicast outputs for each of its HMP routes. You can also enable or disable AES encryption and FEC on the multicast outputs for each location.

Important


To configure browser-based multicast using Media Gateway, the Haivision Helper application must be installed on each user’s computer. For more information, see [Multicast Support via Haivision Helper and Multicast Agent](#).

Topics Discussed

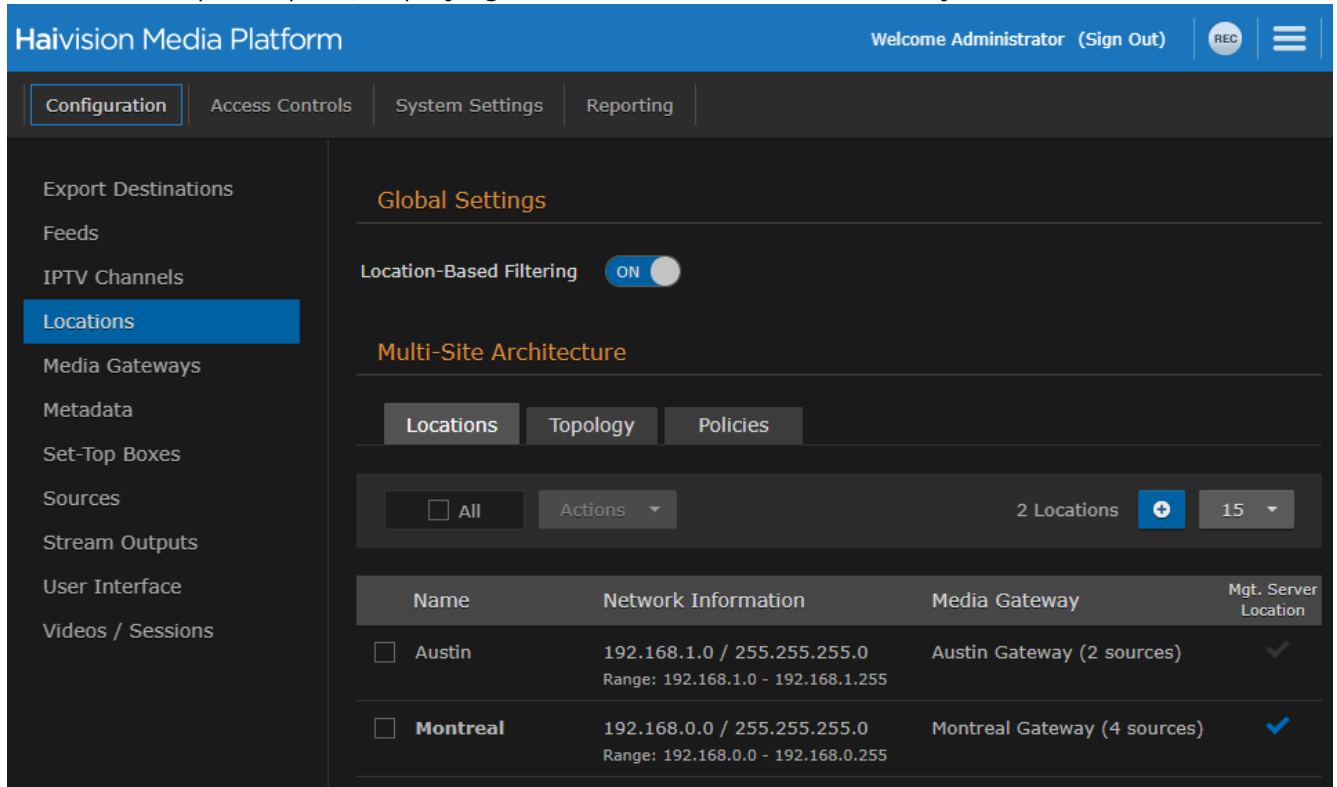
- [Managing Locations](#)
- [Location Settings](#)
- [Locations Topology](#)
- [Locations Policies](#)
- [Troubleshooting Multicast and Diagnostic Tool](#)

Managing Locations

To view and manage locations:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **Locations** on the sidebar.

The Locations pane opens, displaying the list of defined locations, if any.



Global Settings

Location-Based Filtering

Multi-Site Architecture

Locations Topology Policies

All Actions 2 Locations + 15

Name	Network Information	Media Gateway	Mgt. Server Location
<input type="checkbox"/> Austin	192.168.1.0 / 255.255.255.0 Range: 192.168.1.0 - 192.168.1.255	Austin Gateway (2 sources)	<input checked="" type="checkbox"/>
<input type="checkbox"/> Montreal	192.168.0.0 / 255.255.255.0 Range: 192.168.0.0 - 192.168.0.255	Montreal Gateway (4 sources)	<input checked="" type="checkbox"/>

3. (Optional) Disable location-based filtering of content by clicking the Location-Based Filtering toggle **OFF**.

Note

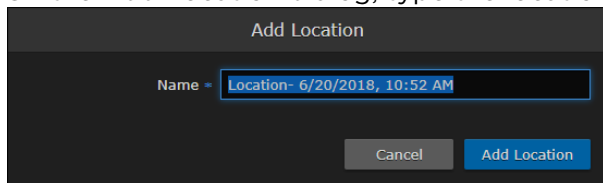
Location-based filtering restricts visibility of sources in Portal and IPTV views for all clients (browser and Haivision Play STBs) based on viewer location for all non-administrator roles. For example, if a source is sent to a Media Gateway at the Montreal location and a user is in the Austin location, the source does not appear in the Portal or IPTV section of the HMP browser. (The Library view is not affected.) If the user then travels to the Montreal location and signs in to HMP, the source appears for the user to view.

4. Check the checkbox under Mgt. Server Location to identify the location of the HMP management server.

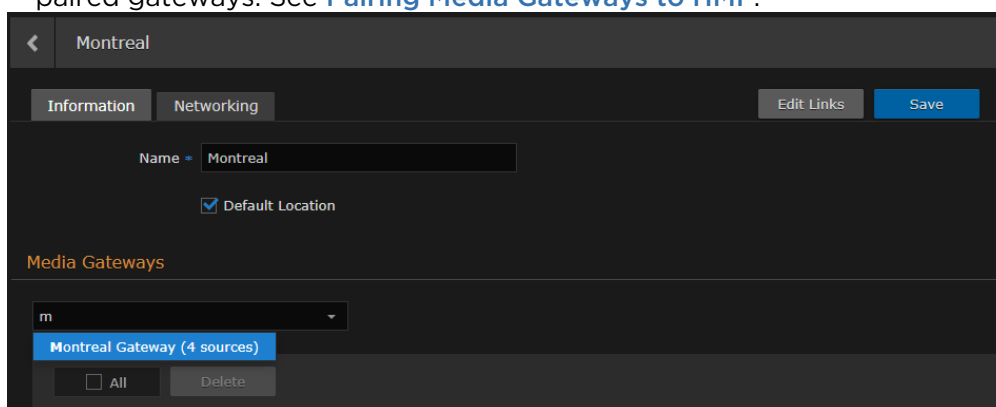
To add a site location:

1. From the Locations pane, click the  icon.

- On the Add Location dialog, type the location name in the Name text field.



- Click **Add Location**.
- On the Location Information pane:
 - Optionally, edit the location name.
 - Optionally, set the location as default by checking the Default Location checkbox (see [Location Settings](#)).
 - To add Media Gateways at the locations, type the first few characters of the gateway name in the Media Gateway field and select the name from the auto-complete drop-down list of available paired gateways. See [Pairing Media Gateways to HMP](#).



- Click the **Networking** tab to configure network settings and multicast playback.
 - For details on each setting, see the "Networking" tab in [Location Settings](#).
 - To specify additional IP addresses and subnet masks for the location, click **+ Network**.
 - If licensed on your system, to specify additional multicast addresses and subnet masks for the location, click **+ Multicast Range**.

6. Click the **Save** button.

Tip

Clicking the **Edit Links** button navigates to the Location Topology pane with the location selected.

Location Settings

Note

If streams are currently active, altering any of the location settings may result in stream interruption.

The following table lists the Location configuration settings:

Information Networking

Setting	Default	Description
Mgt. Server Location (checkbox)	—	Select this location as the HMP management server. The auto-generated routes on the gateway assigned to this location include a loopback destination to HMP.
Name	—	Enter a name for the location. This name is selectable on the Locations list.

Setting	Default	Description
Default Location	Disabled	Select this location as the default. The default location's Media Gateway is used when a user whose IP is not in any of existing location ranges accesses HMP. The default location is displayed in bold in the Locations list.
Media Gateways	none	(Optional) Select a gateway that delivers video to the location from the list of paired Media Gateways (if available). See Pairing Media Gateways to HMP .

Information [Networking](#)

Setting	Default	Description/Values
HMP Connection Mode	Rendezvous for regular HMP systems, Listener for HA cluster configurations	<p>(Management Server Location only) The gateways in the location set to "Mgt. Server Location" have an extra SRT destination/output to be used by HMP for recording purposes. This setting allows you to specify the SRT connection mode to use between HMP and the recording output on HMG:</p> <ul style="list-style-type: none"> • Rendezvous • Listener • Caller <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <ul style="list-style-type: none"> • When HMP is in High Availability (HA) mode, the HMP Connection Mode is Listener (read-only). • If there is a conflict between HMP and HMG connection modes (i.e., if the selected values do not match), the connection mode defaults to Rendezvous. </div>
Link Connection Mode	Any	<p>Select the link connection mode between locations on your network:</p> <ul style="list-style-type: none"> • Any • Listener • Caller
Outputs	Muxed HLS and Variant HLS enabled	<p>Configure the recording outputs generated for each multi-site live source in each location to which they are routed:</p> <ul style="list-style-type: none"> • Muxed HLS • Variant HLS • SRT <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <ul style="list-style-type: none"> • Uncheck the first two boxes to disable either or both of the Muxed HLS (HLS v3) and/or Variant HLS (HLS v4) outputs. • Or check the third box to enable SRT. This configures the Location so that STBs connect to a generated SRT Listener output on HMG (instead of consuming HLS). SRT-capable STBs in that Location then prefer SRT over HLS and be returned a suitable endpoint on the local HMG. </div>
SRT Port Range	31000-31999	<p>Specify the port range to use for your SRT routes between HMP and connected Media Gateways at this location.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>Each route uses an incrementing port. If an upper bound is defined and is lower than the number of ports needed, route outputs are not created and user service is impacted. Unbounded is recommended.</p> </div>

Setting	Default	Description/Values
SRT Listener Port	51000-51999	<p>If SRT is selected in the Outputs field, specify the port range to use for SRT listener routes between HMG and connected STBs at this location.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>⚠ Note</p> <p>Each route uses an incrementing port. If an upper bound is defined and is lower than the number of ports needed, route outputs are not created and user service is impacted. Unbounded is recommended.</p> </div>
SRT Latency	500	<p>(Optional) Specify the SRT output latency in milliseconds.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>⚠ Note</p> <p>To avoid playback issues, we recommend latency values from 500 to 2500 milliseconds.</p> </div>
HLS Segment Duration	10	<p>(Optional) Duration to balance low latency, tune-in time, and stream buffering (range = 1-15 seconds). In the case of HLS live, the duration must be no greater than 15, or it takes too long for the playlist to become available and the initial request is forced to time out.</p>
Bandwidth Limit	—	<p>(Optional) Maximum bandwidth in Mbps to control the rate of outbound traffic to this location.</p>
UDP ToS	0x88	<p>(Optional) Enter the desired UDP Type of Service value in hex format (0x00-0xFF).</p>
IP Address/ Mask	—	<p>In the first field, enter an IP address for the location. This is a unique IPv4 address in dotted-decimal format (xxx.xxx.xxx.xxx). To specify a subnet mask for the location, enter a netmask in the second field, either in dotted-decimal format (e.g., 255.255.0.0) or CIDR notation. A subnet mask is a 32-bit mask used to divide an IP address into subnets and specify the network's available hosts. You can specify multiple IP addresses or subnet masks for a location.</p>
Multicast Address/ Mask	—	<p>If licensed on your system, for multicast delivery, specify the multicast address and subnet mask for the location. To disable multicast, leave Multicast Address empty.</p>
Multicast AES+FEC	Disabled	<p>Check this checkbox to enable AES (Advanced Encryption Standard) and FEC (Forward Error Correction).</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #e8f5e9;"> <p>✔ Tip</p> <p>Typically you might turn off encryption due to interoperability issues with non-Haivision devices.</p> </div>
Disable Unicast Fallback	Disabled	<p>Check this checkbox to prevent users from falling back to HLS streaming if there are problems with the multicast. The default behavior is to give up on a multicast stream that can't be received and go back to regular HLS viewing so that the video can always be seen. This adds latency to the stream but in small user environments doesn't really have other negative effects. However, in large user environments where large numbers of users have trouble with multicast, the load from HLS streaming could overload the network or the server, so you may choose to disable the HLS fallback.</p>
Multicast Port	41000	<p>Specify the port to use for all multicast route destinations in this location.</p>

Setting	Default	Description/Values
Peer To Peer (P2P)	Off	<p>(Must be licensed for peer-to-peer.) Use this switch to enable/disable peer-to-peer playback in this location for HLS streams. To enable peer-to-peer, first a valid P2P key must be populated in the System Settings > Security > Streaming settings. See Configuring HMP for Haivision Peer-to-Peer Video Delivery for more details.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <ul style="list-style-type: none"> • Only applicable for HLS output streams, which can be enabled in the Outputs setting. • Haivision Peer-to-Peer on HMP is currently in Preview Mode. </div>

Locations Topology

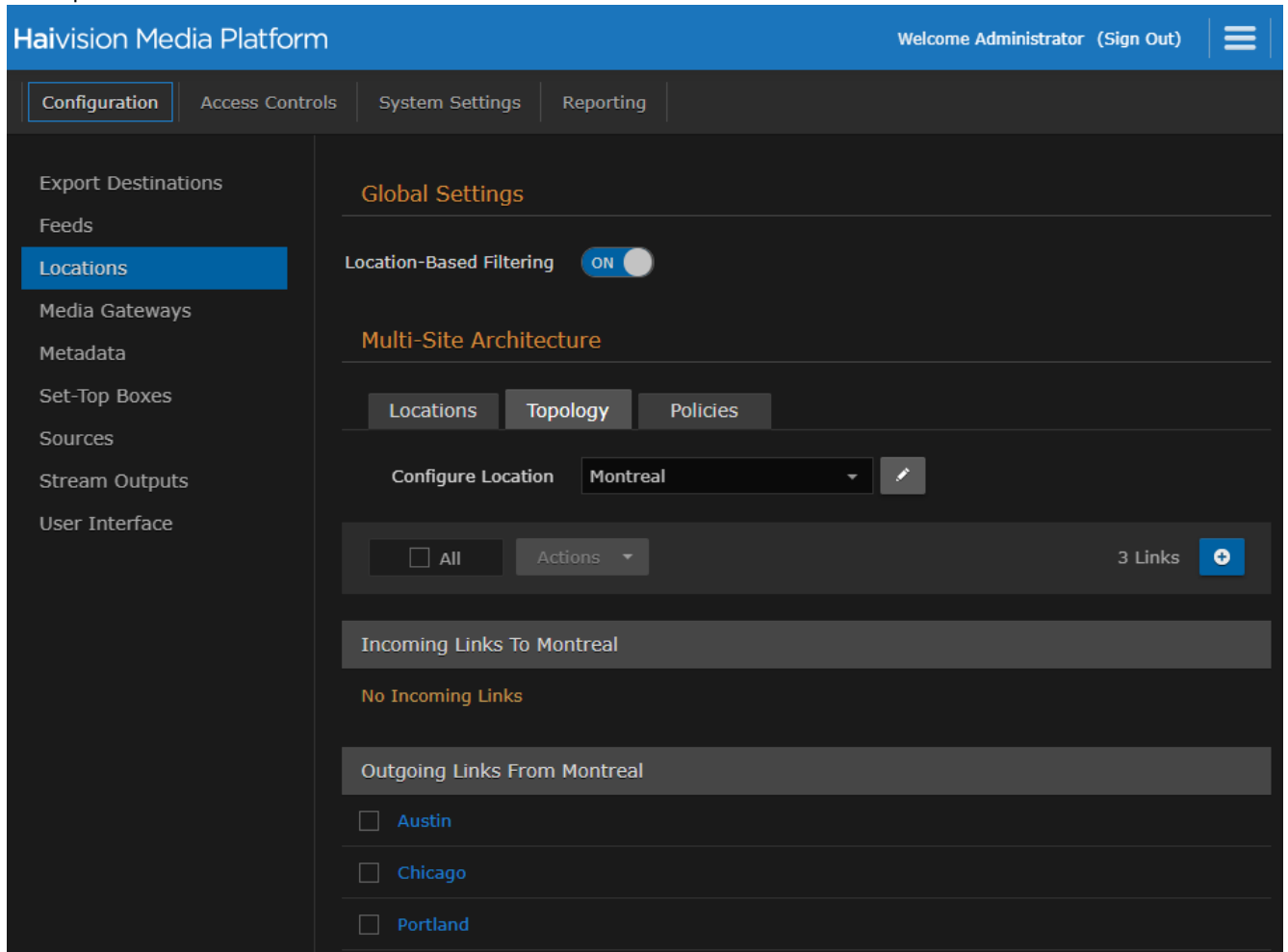
The Locations Topology pane provides administrators a listing of the currently configured Media Gateway locations and shows the incoming and outgoing links between locations. This is designed for large installations where sending streams from the source location directly to *all* other locations is not appropriate or efficient.


By default, HMP automatically distributes sources from the primary HMP server. From the Locations Topology pane, administrators can configure the incoming and outgoing links between locations to control the flow of video from site to site. From here, you can add, edit, and delete links.

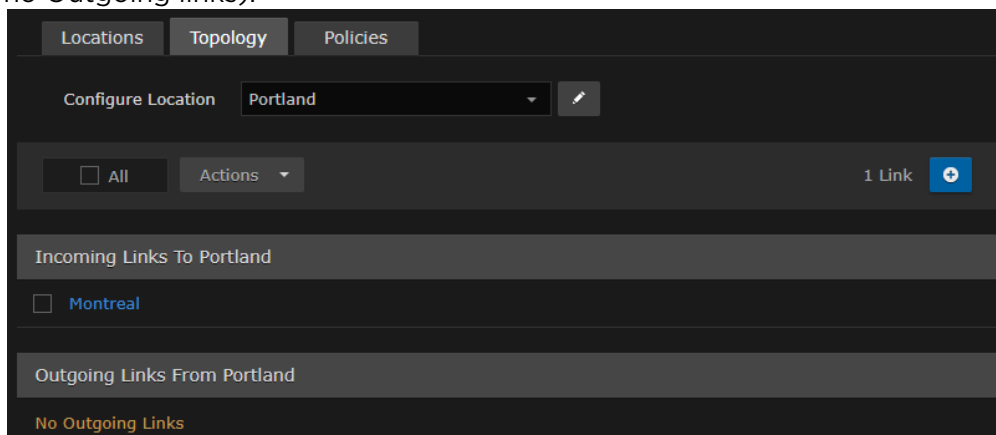
To view and configure locations topology:


1. On the Locations pane, click the **Topology** tab.
The Locations Topology pane opens, displaying the list of Incoming and Outgoing links for the selected location, if any. The default location is automatically selected, as shown in the following

example:




- To filter the list by location, type the first few characters of the location name in the Configure Location search field and then select the name from the auto-complete drop-down list (if available).
Or click the  icon to open the Locations pane.
- To explore the links to and from the current location, click a location hyperlink. In the previous example, if you click Portland under Outgoing Links from Montreal, the pane switches to Portland for the Location and shows the defined links (in this example, an Incoming link from Montreal, but no Outgoing links).



4. Or you can click the  icon to navigate to the Location Information pane for the currently selected location. (See Step #4 in [Managing Locations](#).)

To add or edit a link to or from the current location:

1. From the Locations Topology pane, click the  icon.
2. On the Add Link dialog, select the direction and location.

3. Optionally, you can override the default SRT ToS and SRT Latency values.

 **Important**

The two sides of an SRT connection must use the same ToS values (configured in hex format). If there is a discrepancy between locations, the receiving location defaults to the sending location's ToS value.

4. To enable multicast-enabled network links between locations (i.e., to avoid duplicate streams on the network), check the Multicast Routing checkbox.

 **Tip**

Typically, if your gateways are scattered, this should be kept off, but if your gateways are in one building, enable Multicast Routing.

 **Note**

When editing a link, its direction and location selection cannot be modified; only Multicast Routing can be edited.

5. Click **Add Link**.

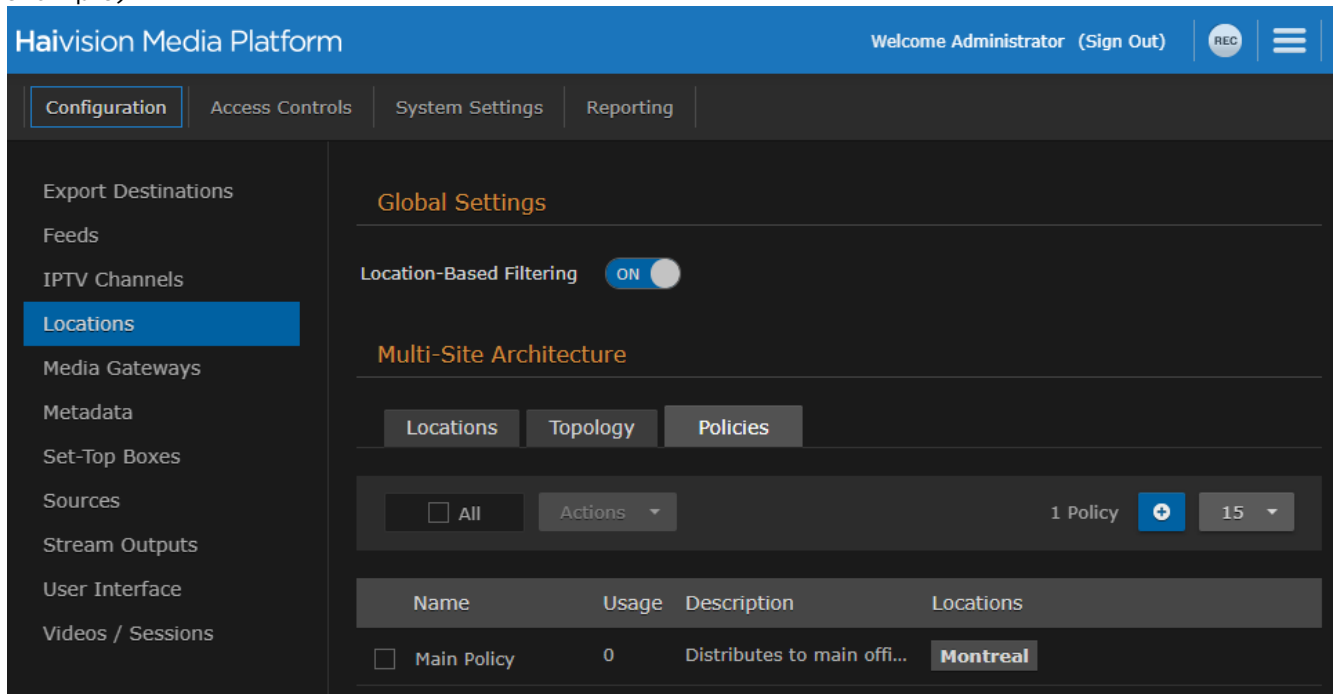
Locations Policies

Distribution policies provide administrators the option to set up selective stream distribution. Each distribution policy contains a list of Media Gateway locations (e.g., NYC, Chicago, Montreal) to which live sessions and scheduled events are sent. Content Creators who wish to limit the distribution of a session or live event to specific locations can simply apply the appropriate distribution policy.

By default, new distribution policies include the default location, so that authenticated users in locations that are not specifically included in the distribution policy are still able to receive the stream.

To view and manage locations policies:

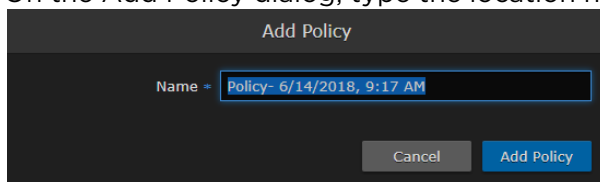
1. On the Locations pane, click the **Policies** tab.
The Locations Policies pane opens, displaying the list of defined policies, if any (see following example).



For each policy, the list shows the name, usage (i.e., the number of times the policy has been selected for a session), the description, and selected locations.

To add a location policy:

1. From the Locations Policies pane, click the **+** icon.
2. On the Add Policy dialog, type the location name in the Name text field.

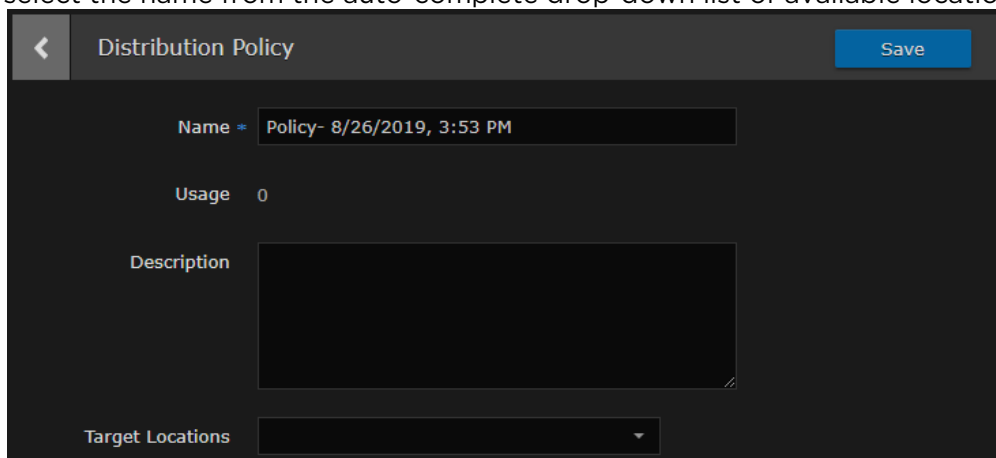


3. Click **Add Policy**.
4. On the Distribution Policy pane, you can edit the policy name, enter a description, and configure its list of target locations.

✓ Tip

It is a good idea to provide a clear description of each policy to guide Content Creators as to which policy to use for different scenarios.

- To select a target location, type the first few characters of the location name in the field and then select the name from the auto-complete drop-down list of available locations.

A screenshot of a mobile application interface for configuring a "Distribution Policy". The screen has a dark background. At the top left is a back arrow icon, and at the top right is a blue "Save" button. Below the title bar, there are four main sections: 1. "Name" with a text input field containing "Policy- 8/26/2019, 3:53 PM". 2. "Usage" with a numeric input field containing "0". 3. "Description" with a large, empty text area. 4. "Target Locations" with a dropdown menu that is currently empty.

- Click the **Save** button. The policy is then added to the list.
- To configure multiple policies, repeat Step 1 through Step 6. These policies are now available in the Sessions/Events Information pane for Content Creators to select.

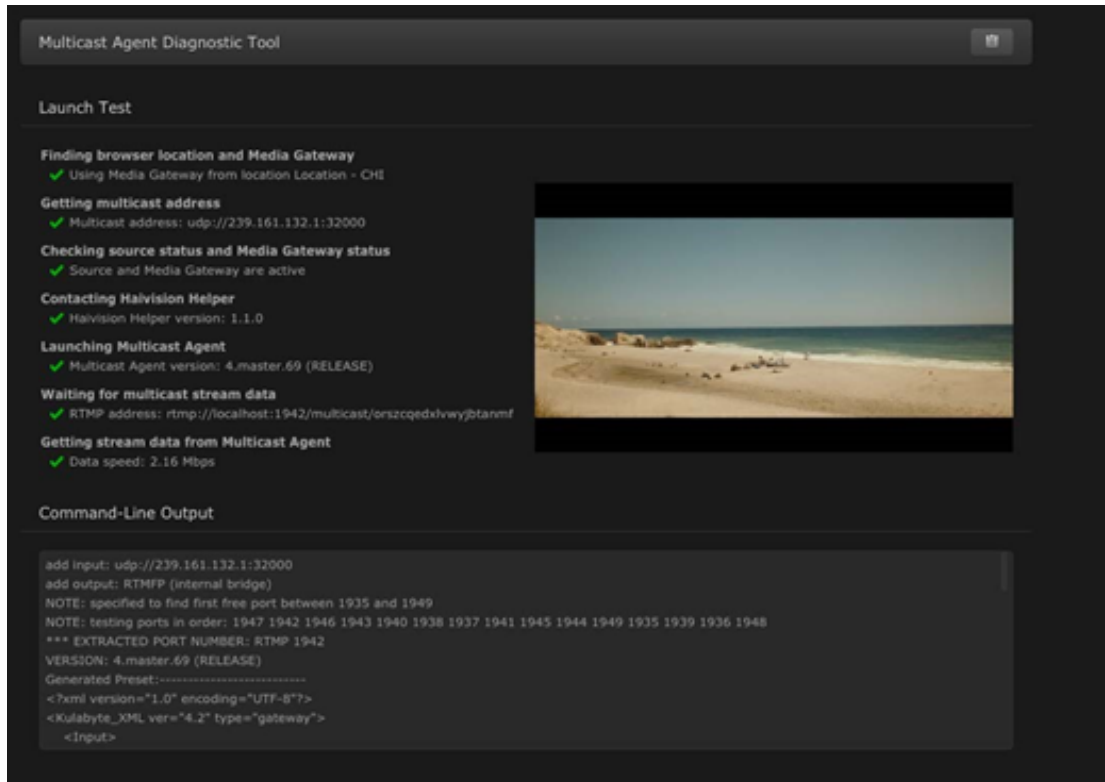
Troubleshooting Multicast and Diagnostic Tool

Below is a listing of basic troubleshooting questions for setting up HMP-Media Gateway pairings.

- Are HMP and the Gateways properly configured?
 - Is multicast agent licensed?
- Is the source multicast enabled and provisioned?
- Is the playback device a supported Mac or PC?
 - Is the latest Haivision Helper installed on the Mac/PC?
- Is the playback device on a multicast enabled network/segment?
 - Is the device on WiFi?
 - Is HMP configured for unicast fallback; is that working?
- When you join the event, do you see "Launching multicast agent"?
- Right-click the video, and click "View Multicast Agent Diagnostic Tool". If you see video here, you know multicast is working.
- Automatic fall-back to unicast (when necessary)
 - Smartphones and tablets don't (typically) support multicast
 - Network segments that don't support multicast (WAN gaps, WiFi)
 - MAC/PC without the Helper installed (or problem with Helper)

Multicast Agent Diagnostic Tool

On HMP desktop sessions and source players, you can access a Multicast Agent Diagnostic Tool pane by right-clicking on any player and clicking “View Multicast Agent Diagnostic Tool”, which causes the tool to open in a new tab. Tests done by the diagnostic tool use the source that was in the player that was clicked in this way.



When the Multicast Agent Diagnostic Tool opens, it performs a single test launch of the Multicast Agent and reports any failures due to bad HMP or user configuration, network issues, or other problems. It launches the Multicast Agent the same way that the normal HMP player does, but performs additional checks to help isolate problems with a multicast environment.

The pane has a **Copy to Clipboard** button that copies test results in a readable text format for easy sharing.

Pairing Media Gateways to HMP


During setup, administrators can pair HMP with one or more Haivision Media Gateways to use the gateway as a proxy cache for media hosted by HMP. Media Gateway is a video streaming solution that gathers and distributes video streams to and from multiple locations.

HMP integration with Media Gateways is used to distribute video to distant site locations, typically pairing a single HMP server with Media Gateway appliances at each location. The Media Gateways provide a network of caching for HMP live streaming and on-demand videos. Users at each location watch video from their local gateway device (although they do not interact directly with the gateway).

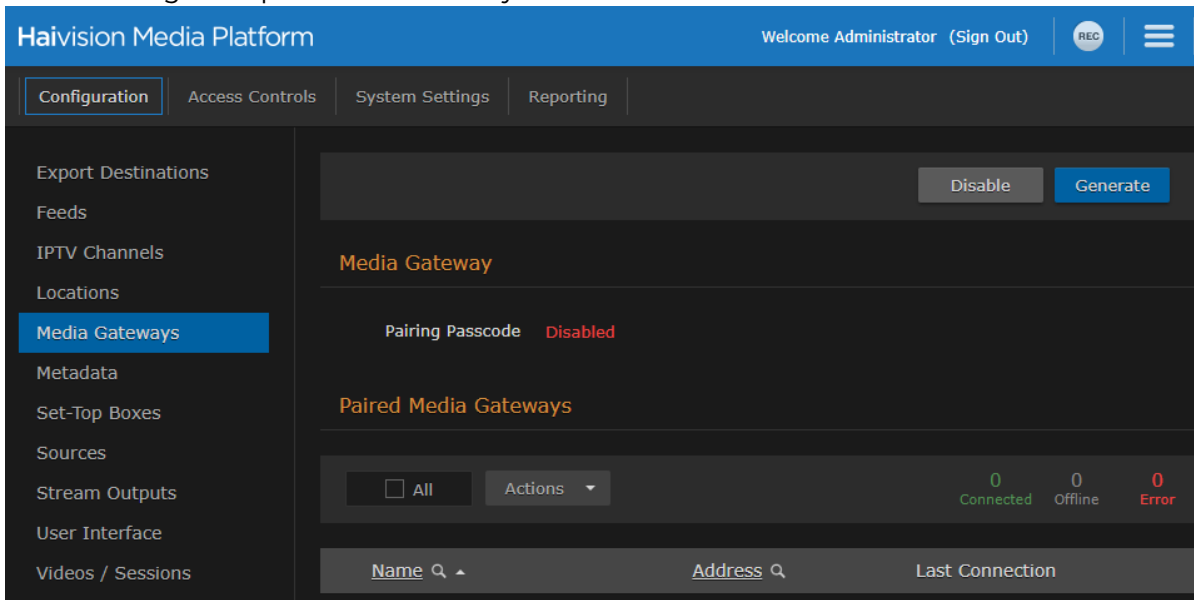
Note

- An HMP can be paired with multiple Media Gateways, but a Media Gateway can only be paired with one HMP.
- Pairing HMP with multiple Media Gateways requires a Multi-site eCDN license.

To view and manage gateway pairings:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **Media Gateways** on the sidebar.

The Media Gateways pane opens, displaying the list of paired media gateways for your platform, if any. The following example shows a new system.



Note

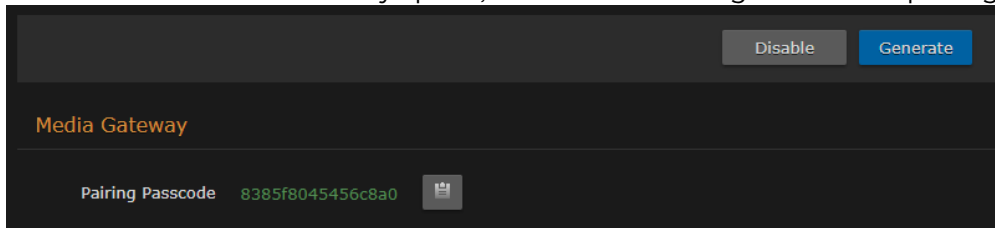
Media Gateway devices initiate outbound requests to HMP to avoid issues with firewall transversal. By default, the HMP pairing passcode is disabled as a security measure, meaning that HMP does not accept any pairing requests.


Tip

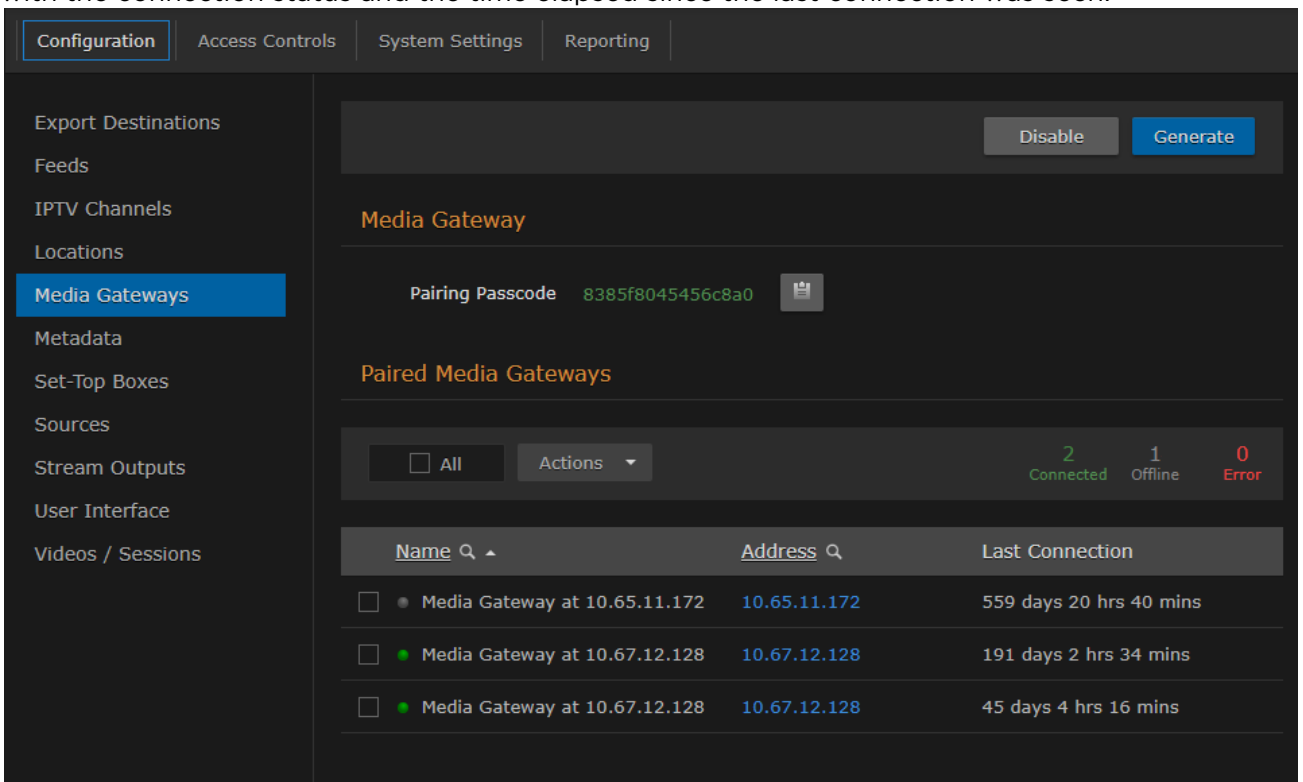
- Setting up the pairing requires steps from both the HMP and Media Gateway Web interfaces.
- You can use the same Pairing passcode to set up multiple gateway pairings.

To add a gateway pairing:

1. On the HMP's Media Gateways pane, click **Generate** to generate the pairing passcode.



2. Click the  icon to copy the passcode to the clipboard.
3. Make note of the HMP address and port. If there is a cross-domain address, make a note of it as well.
4. On the Media Gateway's Administration page, click **Configuration** on the toolbar and then click **Media Platform** on the sidebar.
 - In the Gateway section of the Settings pane, enter the Media Gateway information.
 - In the Media Platform section of the Settings pane, enter the HMP information that you noted earlier and paste the pairing passcode into the Passcode field.
5. Click **Pair**. For more details, refer to the [Media Gateway User's Guide](#).
6. Back on the HMP web interface:
 - On the Media Gateways pane, this gateway is now listed in the Paired Media Gateways list, along with the connection status and the time elapsed since the last connection was seen.



Tip

You can filter the list by selecting either **Connected**, **Offline**, or **Error**. You can also click the gateway IP or hostname (blue) link to open the Media Gateway Web interface in a new browser tab.

- On the Locations Information pane, this gateway is now available for selection from the list of paired Media Gateways. (See Step #5 on [Managing Locations](#).)
7. After you finish pairing all desired Media Gateways, on the HMP Media Gateways pane, click **Disable** to block any new pairing requests.

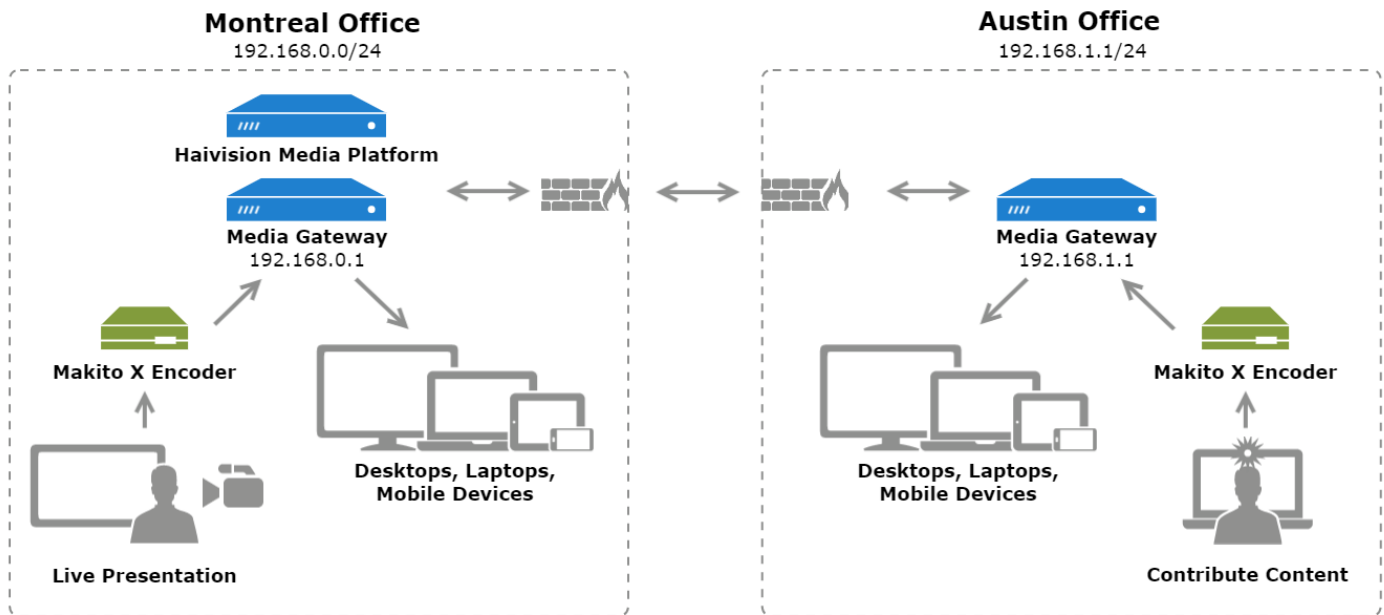
Configuring Multi-Site Live Distribution

Haivision Media Platform works with Media Gateway to support live video distribution across a multi-site environment. This section discusses how to integrate the Media Gateway into HMP for extending the reach of your video network. After a Media Gateway and HMP are configured properly, the system ensures that both live and on-demand video is available to users based on their location on your network and that bandwidth consumption is minimized between network hops.

Important

Before you start, you need to plan your network. We highly recommend that you map out your locations in a network diagram from source to receivers.

The following figure is an example network diagram, which is also referred to in the subsequent procedure:



To configure multi-site live distribution:

1. Pair one or more Media Gateways with your HMP, following steps in [Pairing Media Gateways to HMP](#). Any paired gateways are listed on the (HMP) Media Gateways list. From the above example,

the two Media Gateways are paired to the HMP:

Paired Media Gateways

All Actions ▾ 2 Connected 0 Offline 0 Error

Name	Address	Last Connection
<input type="checkbox"/> Austin Gateway	192.168.1.1	< 1 min
<input type="checkbox"/> Montreal Gateway	192.168.0.1	< 1 min

Tip

You can use the same pairing passcode while pairing multiple gateways. We recommend that you disable the passcode after all gateways have been connected. It can always be turned back on to add a new gateway to the network

- On HMP, create Locations, mapping each with a Media Gateway. For details, see [Configuring Locations](#). Your locations should represent a network where you have a group of users that should receive their video from a particular paired gateway. There can only be one gateway per location. Also select the Mgt. Server Location, i.e., the location of the Haivision Media Platform. From the above example, the two locations are created with appropriate IP address and mask defined for each and the Montreal location is set as the Mgt. Server Location.

Multi-Site Architecture

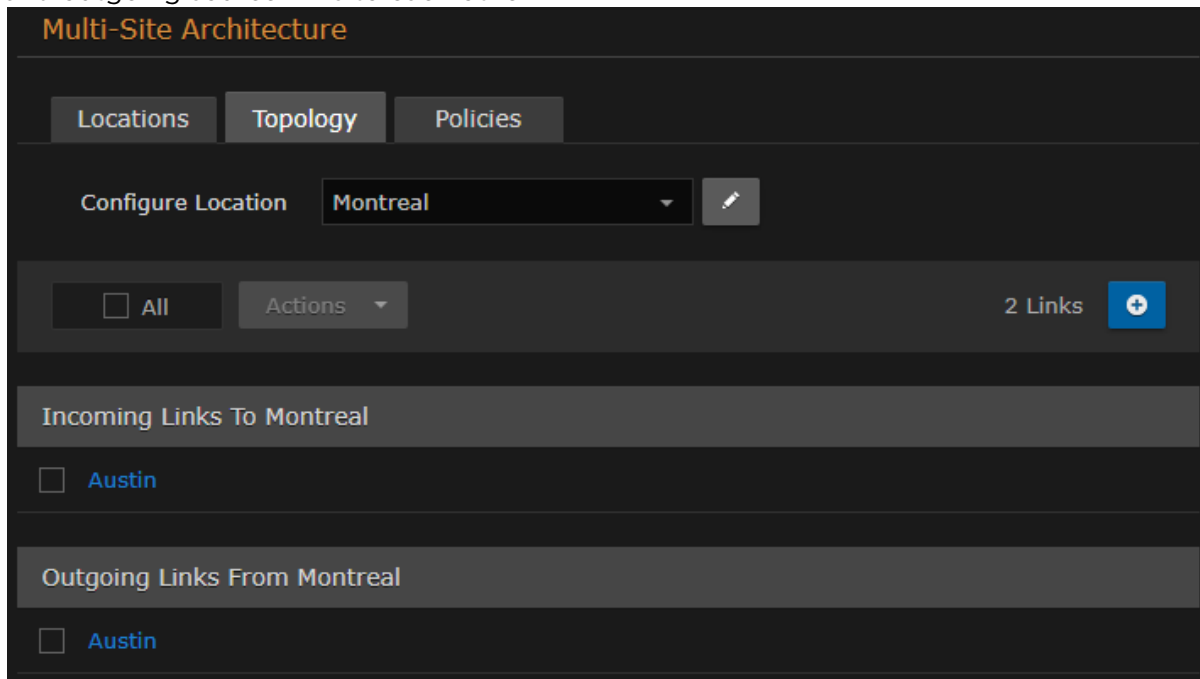
Locations Topology Policies

All Actions ▾ 2 Locations + 15 ▾

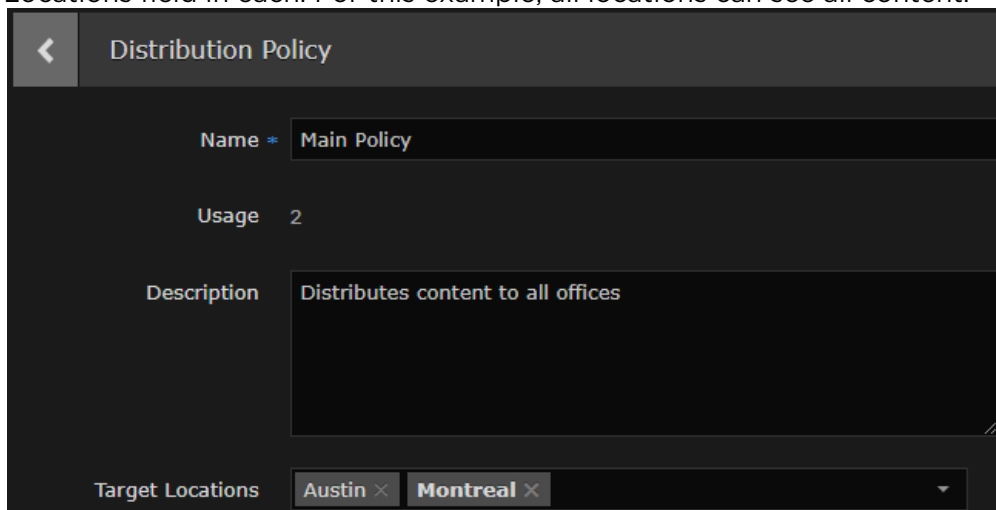
Name	Network Information	Media Gateway	Mgt. Server Location
<input type="checkbox"/> Austin	192.168.1.0 / 255.255.255.0 Range: 192.168.1.0 - 192.168.1.255	Austin Gateway (0 sources)	✓
<input type="checkbox"/> Montreal	192.168.0.0 / 255.255.255.0 Range: 192.168.0.0 - 192.168.0.255	Montreal Gateway (0 sources)	✓

- On HMP Topology list, configure the network topology of your locations; that is, the ingoing and outgoing connections for each location. For the example shown above, the locations have incoming

and outgoing source links to each other.



- On HMP Policies list, create a distribution policy in accordance with your network. If location-based content filtering for non-administrators is desired, create multiple policies and limit the Target Locations field in each. For this example, all locations can see all content.



- On HMP, create one or more sources, selecting one of the paired Media Gateways as the Receiver. For details, see [Adding and Editing Sources](#). For the example shown above, create a source for each Makito X Encoder stream and use the Montreal and Austin Gateways as the receiver for each respectively.

[Montreal Source](#) [Austin Source](#)

Montreal Source [Austin Source](#)

- At your source encoders, send the streams to the gateway at their corresponding location. For this example, the Makito X Encoder streams are sent to their respective Media Gateway.

[Montreal Source](#) [Austin Source](#)

Montreal Source

Name	Protocol	Destination	Content	Action
Montreal source	TS over SRT	192.168.0.1:1234	Video Audio	None

Montreal Source [Austin Source](#)

Austin Source

Name	Protocol	Destination	Content	Action
Austin source	TS over SRT	192.168.1.1:1233	Video Audio	None

- On HMP, create sessions for the configured sources and assign the appropriate distribution policy for each. See [Adding a Session](#) in the User’s Guide for details. For this example, both sources are added to a single session, the distribution policy sends the content to both locations, and the session starts immediately.

- Based either on the Schedule or "Live" state, multi-site routes are automatically created on the paired Media Gateways. For this example, the routes are created immediately and their status is viewable on each Media Gateway.

Montreal Gateway Route Austin Gateway Route

Node	Name	Protocol	Type	Address	Stream ID	Status
Source	source-receiver	UDP	Unicast	0.0.0.0:1234		●
Destination	Haivision Media Pla...	SRT	Caller	192.168.0.168:31...		●
Destination	hls-output	HLS	Server	https://192.168.0....		●
Destination	hls-output-v3	HLS	Server	https://192.168.0....		●

Tip
 The SRT destination route at the Management Server location is used by HMP for recording the session. Its status is yellow if the session is not actively being recorded.

Montreal Gateway Route Austin Gateway Route

The screenshot shows a configuration window for a source-receiver. The title bar indicates 'source-receiver (2 Destinations)' and 'Uptime: 24m0s'. Below the title bar is a table with the following data:

Node	Name	Protocol	Type	Address	Status
Source	source-receiver	UDP	Unicast	0.0.0.0:1233	●
Destination	hls-output	HLS	Server	https://192.168.0....	●
Destination	hls-output-v3	HLS	Server	https://192.168.0....	●

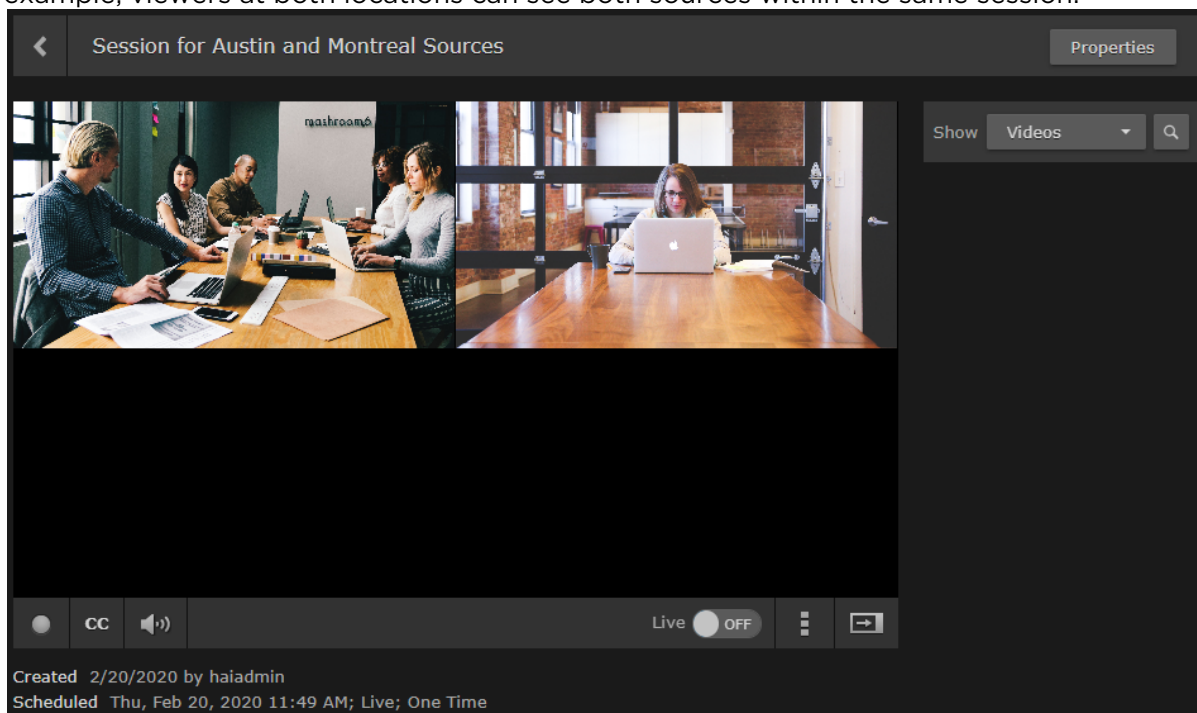
Live multi-site routes are created on all paired Media Gateways when a source belongs to an active session. Specifically, multi-site Gateway routes are created for each unique source when the source belongs to:

- a scheduled session that is inside of the scheduling window
- a scheduled session that is starting within 5 minutes
- a scheduled session that has ended within 5 minutes
- a manually created, unscheduled session (i.e., no end time) that is in the "Live" state

Note
 A scheduled session has active multi-site routes regardless of its "Live" state. All configured gateways receive live streams when a source is made available through a session.

For additional information, please refer to "Multi-site Live Workflow" in the [Media Gateway User's Guide](#).

- The content is now viewable on HMP depending on your location and permission settings. For this example, viewers at both locations can see both sources within the same session.



Defining Metadata

Haivision Media Platform administrators can define metadata with selectable values to identify and store custom metadata. For example, videos, sessions, and sources may be categorized by surgical procedure, course title, geographical location, or patient ID number – whatever makes sense in your environment.

This metadata can be assigned to videos, sessions, and sources. From the Library and Portal, viewers can select metadata keys and values to filter the Videos, Sessions, or Sources list. For details, see [Filtering Lists \(Advanced Search\)](#) in the User’s Guide.

Note

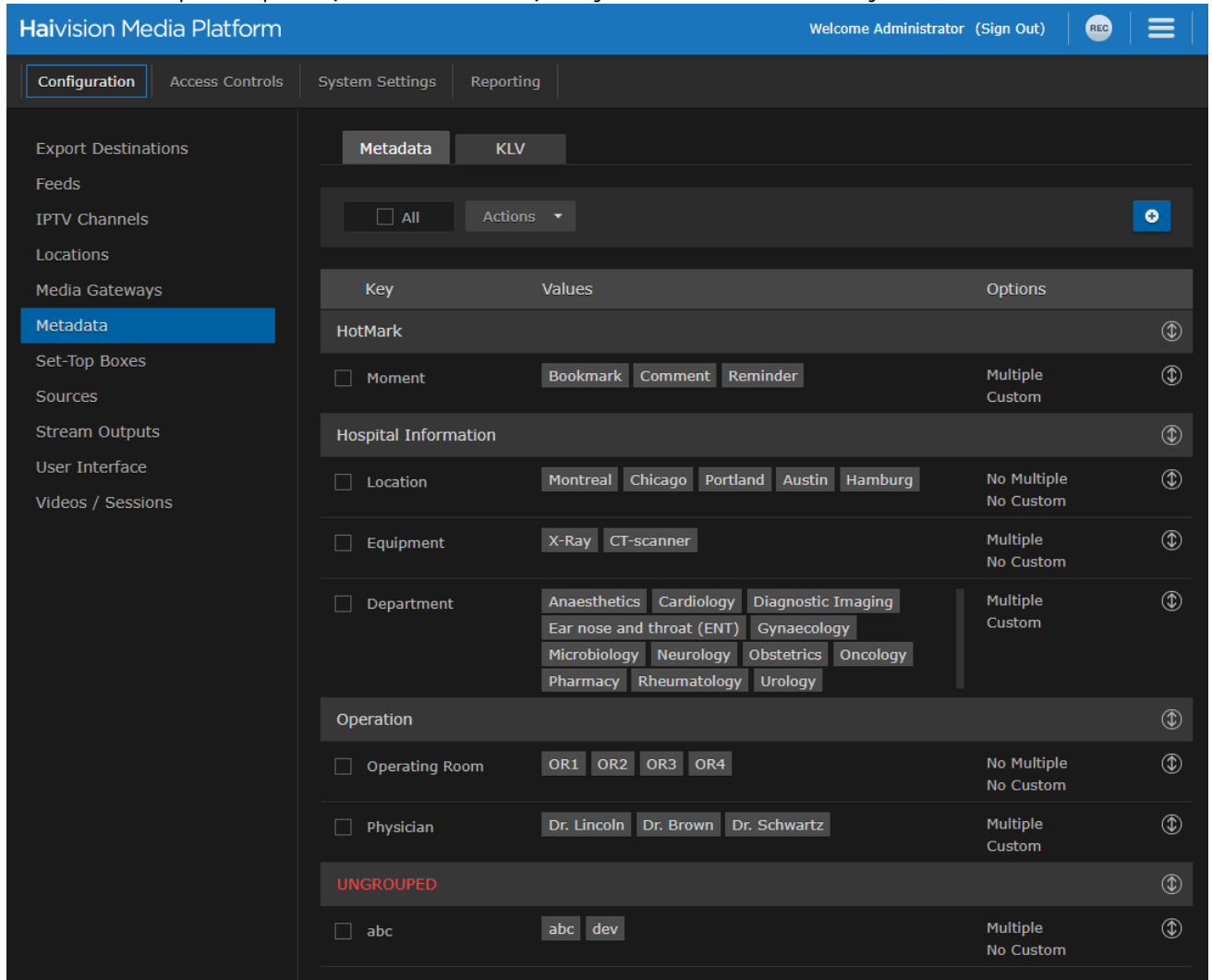
Viewers only see metadata assigned to videos for which they have access.

To help you manage your metadata, you can organize metadata into groups, change the display order of metadata keys within the group, and sort groups within the list of keys. (Metadata cannot be sorted on mobile devices because they do not have the same drag and drop support as desktop browsers.)


To view and configure metadata:

- Click the  icon and select **Administration** from the navigation drop-down menu.

- Click **Configuration** on the toolbar and then click **Metadata** on the sidebar. The Metadata pane opens (as shown below). Any defined metadata keys are listed.



To define metadata:

- On the Metadata pane, click the  icon.

- On the Add Metadata dialog, type in the metadata key (label), for example, Department.

- In the Values field, type in the values for the metadata, one at a time (as shown in the following example). Press Enter after each value.

Note

By default, users are able to enter multiple values, but not custom (i.e., their own) values when assigning metadata to videos, sessions, and sources.

To remove a value, mouse over the value and click the **X** icon.

- To use the Metadata for HotMarks, check the checkbox. Note that HotMarks serves as the group for the metadata.

-or-

In the Group field, type in the group for the metadata.

Add Metadata

Key *

Values * × × ×

Use for HotMarks

Group

Select Multiple Values

Enter Custom Values

✔ **Tip**

If you do not assign a group to the metadata or select it for use with HotMarks, it is listed as UNGROUPED.

Key	Values	Options
UNGROUPED		↕
<input type="checkbox"/> Department 2	<input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Orthopedics"/>	Multiple No Custom ↕

5. Check the checkboxes to modify the default settings for Multiple Values and Custom Values as required. For more information see [Metadata Settings](#).
6. When you have finished typing in the values, click **Add Metadata**. The new metadata key is added to the Metadata list.
7. To change the display order of metadata keys within a group or groups within the Metadata list, click the ↕ icon for the metadata key or group and drag it to the adjust the order of the list. The metadata key being sorted (dragged) is blanked out and outlined with a blue dotted border.

Key	Values	Options
Hospital Information		↕
<input type="checkbox"/> Location	<input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Montreal"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Chicago"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Portland"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Austin"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Hamburg"/>	No Multiple No Custom ↕
<input type="checkbox"/> Equipment	<input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="X-Ray"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="CT-scanner"/>	Multiple No Custom ↕
<input type="checkbox"/> Department	<input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Anaesthetics"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Cardiology"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Diagnostic Imaging"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Ear nose and throat (ENT)"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Gynaecology"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Microbiology"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Neurology"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Obstetrics"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Oncology"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Pharmacy"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Rheumatology"/> <input style="background-color: #444; color: #fff; padding: 2px 5px;" type="text" value="Urology"/>	Multiple Custom ↕



Tip

If you select multiple metadata keys to edit, only the Group field is editable.



Important

Deleting a metadata key also removes associated values on all videos, sessions, and sources.

Topics Discussed

- [Metadata Settings](#)
- [Managing KLV Inputs](#)

Metadata Settings

The following table lists the Metadata configuration settings:

Metadata Setting	Default	Description/Values
Key	—	The label for the metadata.
Values	—	One or more default values that can be selected by users for this metadata.
Use for HotMarks	Disabled	Enable to add this metadata to the HotMarks list instead of the general Metadata list.
Group	—	(Optional) The group to assign the metadata to. Grouping helps you organize large numbers of metadata keys and intuitively arrange them for viewers. You can also sort keys within groups and sort groups within the list of keys.
Select Multiple Values	Enabled	Allows users to add more than one value to this metadata key.
Enter Custom Values	Disabled	Allows users to add their own values for this metadata key.

Related Topics

- [Filtering Lists \(Advanced Search\)](#) in the [User's Guide](#).

Managing KLV Inputs




Note

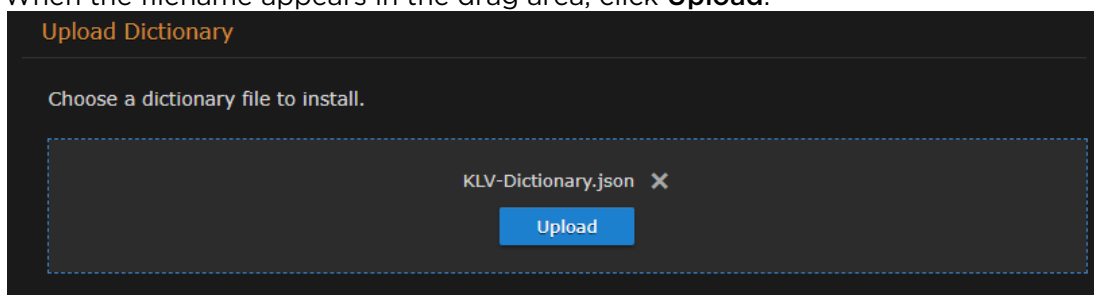
- KLV is a licensed option. For more information, please contact Haivision Sales.
- These topics do not apply to the low-latency player, as a KLV dictionary is only needed for the legacy Flash-based player.

For the legacy Flash-based player, administrators can create and upload a metadata dictionary file to customize and dynamically display KLV metadata to provide context with associated video/audio streams.

To accommodate changes to the KLV dictionary, HMP accepts a library file which translates the KLV data being sent into human readable fields and units of measure. The library file is in JSON format and complies with [MISB RP 0602.2: Annotation Universal Metadata Set](#) and [MISB Standard 0604.1: Time Stamping and Transport of Compressed Motion Imagery and Metadata](#). Administrators can also download and review the currently uploaded KLV dictionary.

To manage KLV inputs:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **Metadata** on the sidebar.
3. On the Metadata pane, click the **KLV** tab.
 - To view the currently installed dictionary, click **Download**. You can then open the file in a text editor to view the KLV dictionary.
 - To remove the currently installed dictionary from your system, click **Remove**.
 - To upload a dictionary:
 - i. Drag a file to the drop area or click **Choose a file** and select the dictionary file to load. For details on the dictionary file format, see [KLV Dictionary Format](#). A sample dictionary file is available on Haivision's Support Portal at: <https://support.haivision.com>
 - ii. When the filename appears in the drag area, click **Upload**.




The dictionary is now loaded. KLV metadata can now be displayed for videos, sessions and sources.

Setting Default Set-Top Box Values

From the Administration screen, you can configure default settings to assign to new set-top boxes registered in the Haivision Media Platform domain. You can also create tags for tag-based configuration of devices.

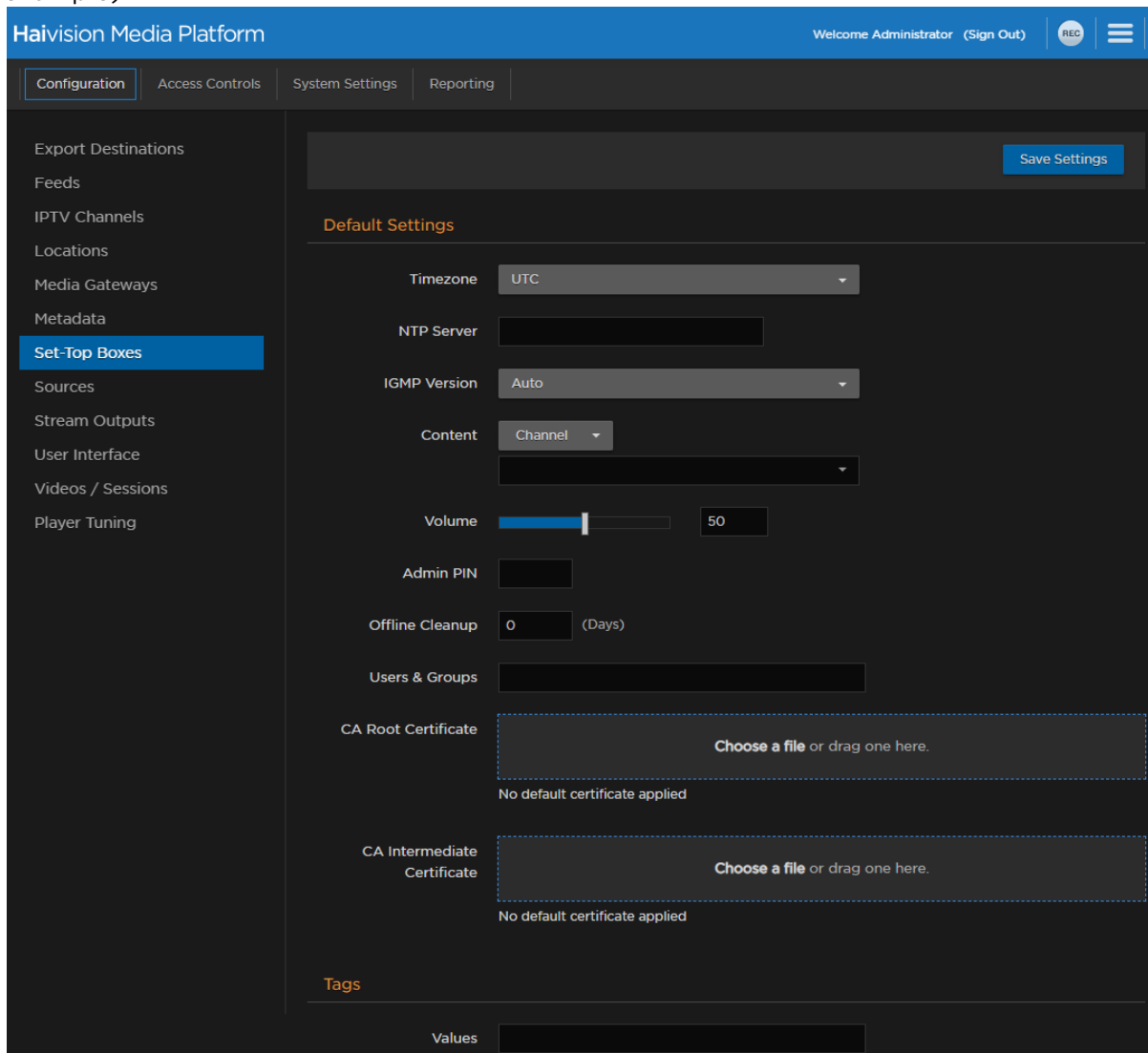
When registering a new set-top box as a device in an HMP domain, it is assigned the default settings. This is useful to control settings such as the channel lineup, volume level, NTP server, and Timezone, the first time the device connects to HMP. You can also load SSL certificates onto the STBs from this screen.

To configure default device settings:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **Set-Top Boxes** on the sidebar.

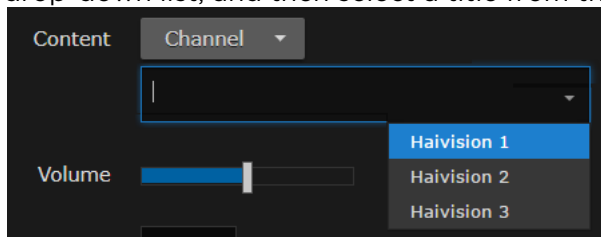
The Set-Top Boxes pane opens showing the device default settings (as shown in the following

example).



3. Enter or select the values to serve as default device settings. See [Device Default Settings](#).

4. To specify the default content type, select either Channel, Videos, Sessions, or Layout from the drop-down list, and then select a title from the detailed list.








5. See [Tagging Devices](#) for details on setting device tags.

6. Click **Save Settings**. The changes take effect immediately and apply to new STBs registered with the server.

Device Default Settings

The following table lists the Device Default settings:

[Default Settings](#) [Device Tags](#)

Setting	Description/Values
Timezone	<p>Initially set to UTC. To modify, select the desired time zone and corresponding city.</p> <div style="border: 1px solid #f0e68c; padding: 5px;"> <p> Note The times are based on hours added to or subtracted from Greenwich Mean Time (GMT).</p> </div>
NTP Server	<p>This is blank the first time you open the (HMP) Devices screen after an upgrade. After setting the default, it is applied to newly registered STBs. To modify, enter the FQDN or IP address of the NTP (Network Time Protocol) Server for the device. Setting this allows the unit to keep the date and time in sync with an NTP server.</p> <div style="border: 1px solid #f0e68c; padding: 5px;"> <p> Note Haivision Play 1000 STBs do not support FQDNs for the NTP server. Use an IP address only.</p> </div> <div style="border: 1px solid #c8e6c9; padding: 5px;"> <p> Tip Generally, it is recommended to use the same NTP server as HMP.</p> </div>
IGMP Version	Initially set to Auto. If required by your system, select IGMPv2 or IGMPv3.
Content	<p>Select the default content type for the device, either channel, videos, sessions, or layouts. Then select the channel, video, session, or layout title from the drop-down list.</p> <div style="border: 1px solid #f0e68c; padding: 5px;"> <p> Note Layouts are not available as default content for Haivision Play 1000 STBs.</p> </div>
Volume	To raise or lower the volume, move the volume slider right or left. Or type in the volume level in the text box.
Admin PIN	<p>(Play 1000 STB only) To set the Admin PIN code, type in a 4-8 digit PIN. When an Admin PIN is set, this locks down Settings screen, and users must enter this PIN to access the STB Settings application. After you save the Default Settings, this becomes the default Admin PIN for any STBs registered in this HMP domain.</p> <div style="border: 1px solid #c8e6c9; padding: 5px;"> <p> Tip If you are not using an Admin PIN, clear the input field (leave it empty) and click Save.</p> </div>
Offline Cleanup	To set the offline cleanup period, enter the number of days. Devices offline for more than the specified cleanup period are removed from the Devices list. To disable automatic cleanup, set to 0 (default).
Users and Groups	Enter the names of defined users and groups to assign access to the STB content.

Setting	Description/Values
CA Root Certificate CA Intermediate Certificate	<p>When using self-signed certificates in your workflow, it is necessary to load the certificates onto each connected set-top box before viewing HMP video streams, downloading latest STB firmware, etc. For new STB installs, this must be completed manually using a USB drive or microSD card. See Connecting the Set-Top Box to your HMP Server for details.</p> <p>However, when updating self-signed certificates on existing operational STBs, use these file input fields to apply a new root certificate and intermediate certificate (if applicable).</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>After updating certificates, an STB reboot is necessary. Issue a reboot command from HMP as described in Controlling Devices.</p> </div>

Default Settings Device Tags


Setting	Description/Values
Values	Enter one or more words or phrases to describe and manage the device. See Tagging Devices .

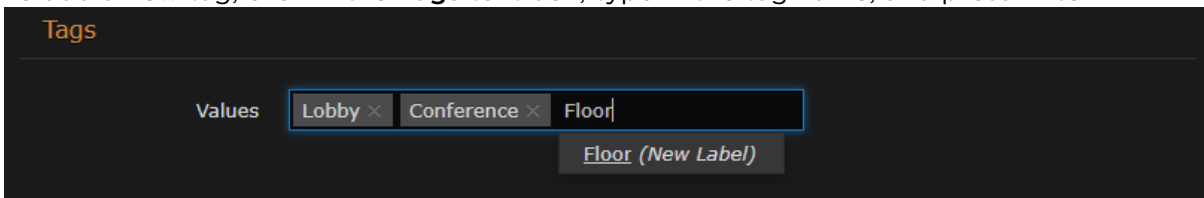
Tagging Devices


Tagging devices facilitates online management of large installations. It provides a helpful way to sort, manage, and schedule devices with a high degree of control over content being sent to individual or groups of devices. Tags are similar to, but more specific than groups and are generally used to describe and manage devices with more granularity. Tag-based configuration is also more powerful than groups because a single device can have more than one tag. Tag-based configuration allows devices to essentially be in more than one group.

After devices are tagged, you can filter by tags to view, edit, or schedule only devices that share selected tags. This is useful to narrow and manage long lists of devices and also makes it easier to locate devices in large installations. (See [Viewing and Managing Devices](#) in the User’s Guide)

To add or delete tags:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **Set-Top Boxes** on the sidebar.
3. Scroll to the bottom to view the defined tags for the HMP domain.
 - To add a new tag, click in the **Tags** text box, type in the tag name, and press **Enter**.



- To remove a tag, mouse over the name and click the  icon.
4. Click **Save Settings**. Keep in mind that the Save Settings button applies to both default settings and tags.

The newly created tags are now available to assign to devices and then to filter the displayed list.

Managing Sources

A *source* is an incoming unicast or multicast video stream or IPTV channel that can be recorded or viewed live. When setting up Haivision Media Platform, you need to define the streaming A/V sources to be available for content creators and other users to view and capture.

When adding a source, you can assign a name, description, IP address and port, and protocol type. By default, the source has an HMP receiver, but for multi-site live distribution, you can associate the source with a Media Gateway receiver. When editing the source information, you can add metadata and change the access permissions of the source.


The supported protocol types are UDP or SRT. With UDP, you can select multicast or unicast streaming. SRT optimizes streaming performance across unpredictable networks, including the public Internet.

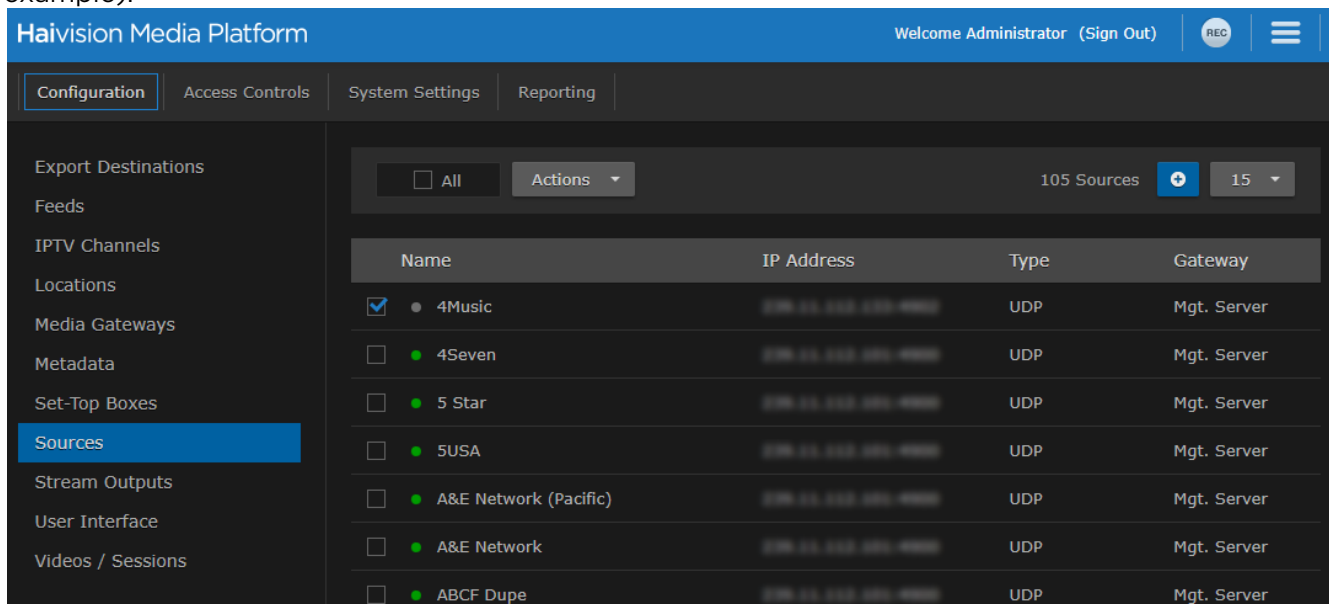
You can also configure the source to display EPG data on Haivision Play Set-Top Boxes from Haivision servers.

Note

Users can view source content before creating a session on the Library screen. See [Previewing Sources](#) in the User’s Guide.

To view and manage sources:

1. Click the  icon and select Administration screen from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **Sources** on the sidebar. The Sources list opens, displaying the list of defined sources for your platform (see following example).



Topics Discussed



- [Adding and Editing Sources](#)
- [Creating a Watermark for a Source](#)
- [Source Settings](#)

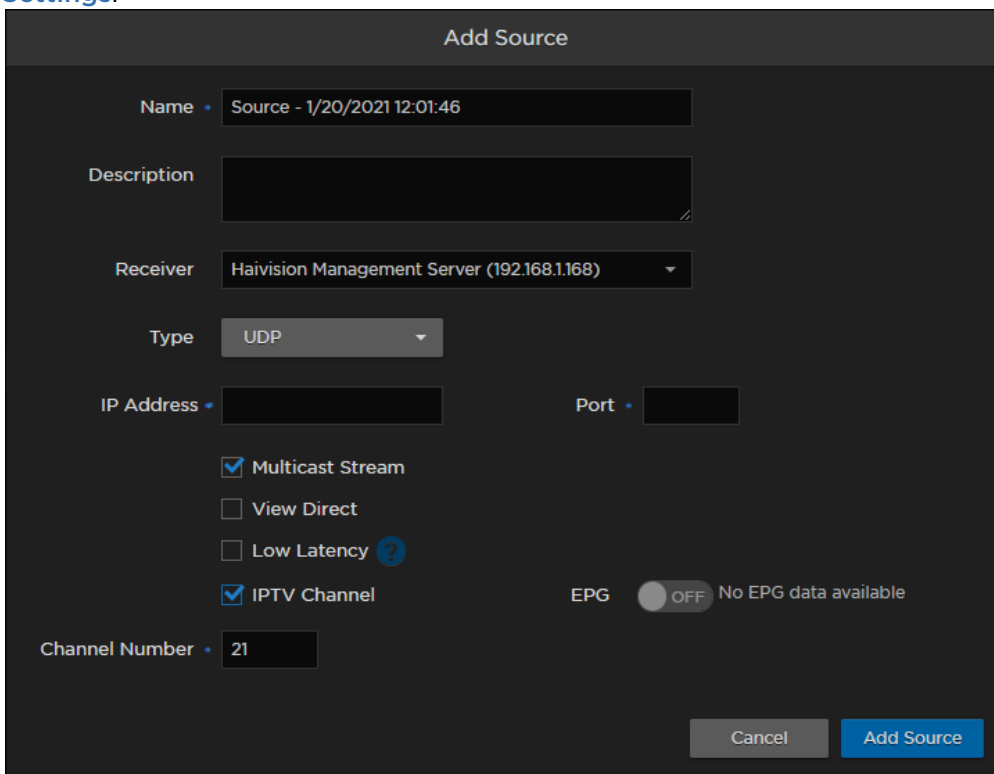
- **Configuring Secure Reliable Transport (SRT) Sources**

Adding and Editing Sources

[Adding a Source](#) [Editing a Source](#)

To add a source:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **Sources** in the sidebar.
3. From the Sources list, click the  icon.
4. On the Add Source dialog, enter a name and other values to define the source. See [Source Settings](#).



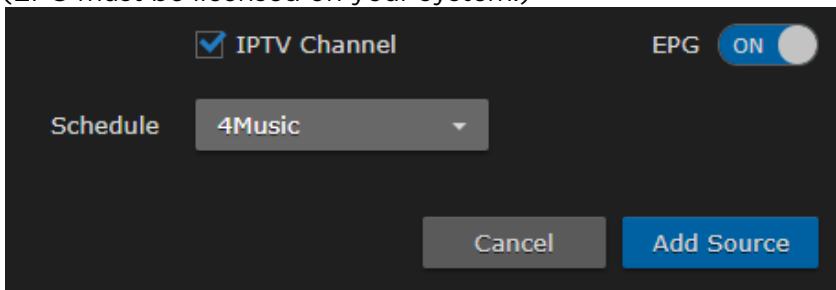
The fields vary depending on the selected Receiver and Protocol Type, and the licensed features.

- To configure a source using the SRT streaming protocol, select SRT for the Type and then fill in the additional fields. For details, see "SRT Settings" in [Source Settings](#).
 - To configure the source for multi-site live distribution, select a Media Gateway from the Receiver list of paired media gateways for your platform (if any, see [Pairing Media Gateways to HMP](#)).
 - Media Gateway also allows you to select RTMP or RTSP sources. For details of these settings, see "RTMP Settings" and "RTSP Settings" in [Source Settings](#).
5. For the Haivision Play Set-Top Box, to use the source URL directly instead of an HLS version, check the View Direct checkbox.
 6. (Live Review licensed systems only) To enable the low-latency player for the source, check the Low Latency checkbox.

Note

- Low latency is currently in Preview Mode.
- Low latency distribution of a unicast stream from HMP uses additional system resources. Only enable this feature for streams with very limited viewership or streams that are always distributed to clients via multicast.
- Closed captions are not supported by the low latency player.

7. To enable the source for IPTV deployment, check the IPTV Channel checkbox, and enter the desired channel number.
8. To display EPG data on set-top boxes, toggle the **EPG** button to **On** and select the Schedule. (EPG must be licensed on your system.)



9. Click **Add Source**.
The new source is added to the Sources list.

Adding a Source **Editing a Source**

To edit sources:

1. Select one or multiple sources in the Sources list.
2. On the Source Information pane, enter or select the values to modify the source.
 - For the steps to edit a source, see [Editing Information and Metadata](#) in the User’s Guide.
 - For the source configuration settings, see [Source Settings](#).

Tip

To configure an SRT source, see [Configuring Secure Reliable Transport \(SRT\) Sources](#).

3. To assign metadata to the sources, click the **Metadata** tab. Metadata keys and values must be pre-defined on your system. See [Defining Metadata](#).
 - On the Source Metadata pane, select the applicable metadata and values from the drop-down lists.

Note

If you select multiple sources and the metadata has mixed (i.e., different) values, a warning appears across the top of the list and the metadata with mixed values are displayed in yellow. For the steps to bulk-edit metadata, see [Editing Information and Metadata](#) in the User’s Guide.

4. To change access permissions, click the **Access** tab and follow the steps in [Sharing Items](#) in the User’s Guide.

5. (For advanced users only.) To change the tuning profile for the source, click the **Advanced** tab and select the profile in the drop-down list.
6. To add/edit a watermark for a source, click the Advanced tab and adjust the Watermarking settings. See [Creating a Watermark for a Source](#) for details.
7. Click **Save**.


Creating a Watermark for a Source

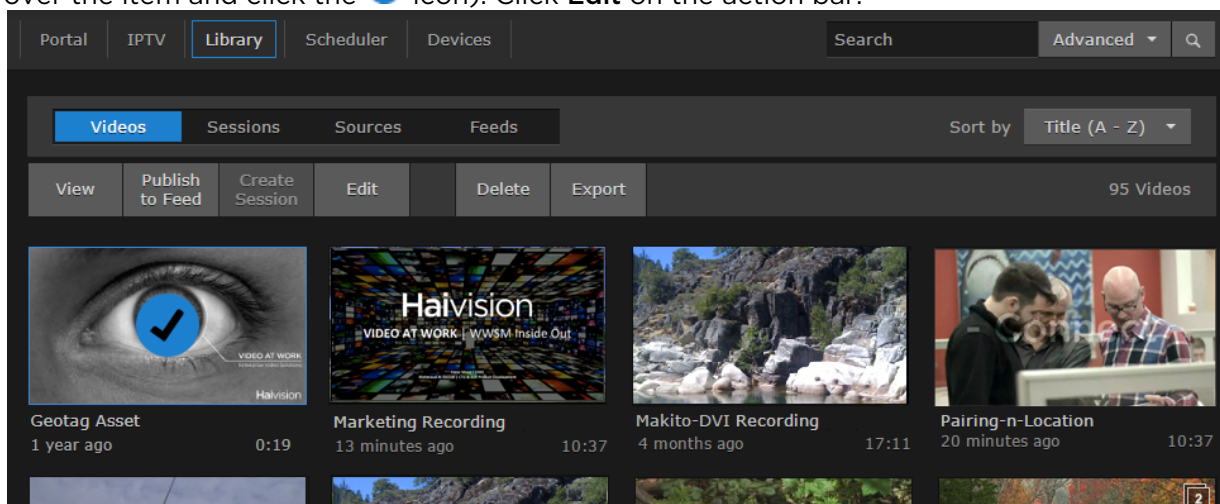
Depending on your role permissions, you can create a watermark for your content to appear in the player.


Note

- Watermarks do not appear in Layouts sent to Haivision Play 2000/4000 STBs.
- Watermarks do not appear on Haivision Play 1000 STBs or Apple iPad browser.

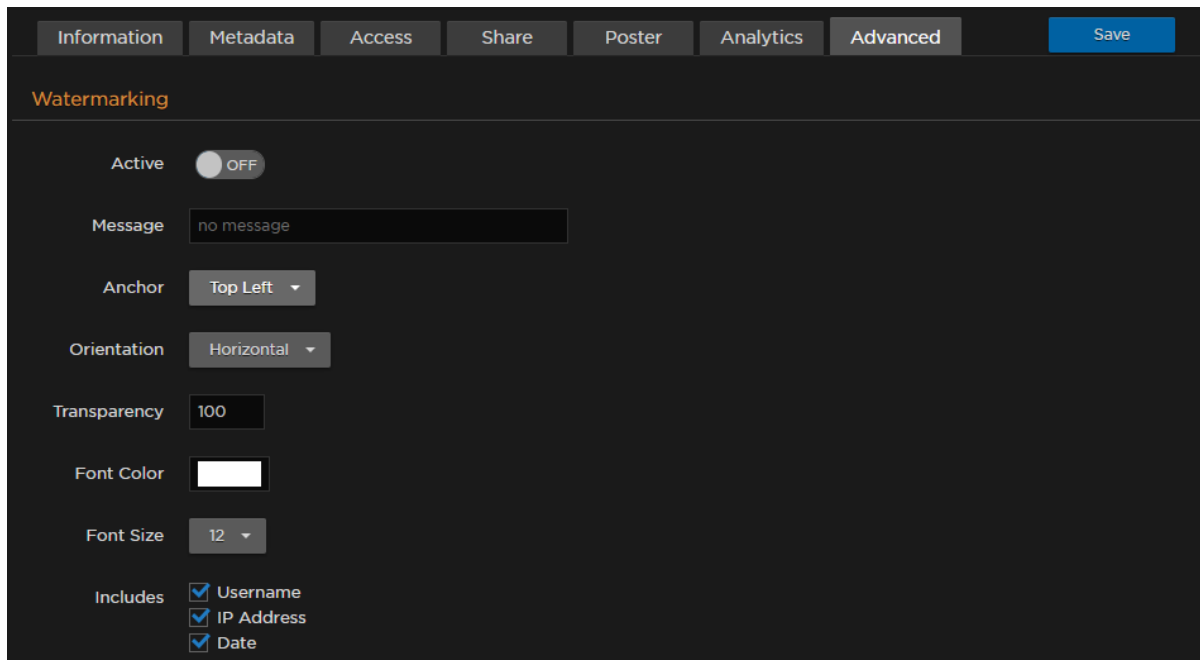
To create a watermark for a session, video, or source:

1. On a list such as the Videos list (shown in the following example), select an item (hover the mouse over the item and click the  icon). Click **Edit** on the action bar.



Or hover the mouse over the item and click the  icon.

2. On the Information pane, click the **Advanced** tab. From here you can:
 - Enable, add, position, and format the watermark.
 - Append the username, IP address, or data/timestamp that the session/video/source starts to be watched.



The screenshot shows the 'Watermarking' settings panel. At the top, there are tabs for 'Information', 'Metadata', 'Access', 'Share', 'Poster', 'Analytics', 'Advanced', and a blue 'Save' button. The 'Watermarking' section is active and contains the following settings:

- Active:** A toggle switch set to 'OFF'.
- Message:** A text input field containing 'no message'.
- Anchor:** A dropdown menu set to 'Top Left'.
- Orientation:** A dropdown menu set to 'Horizontal'.
- Transparency:** A numeric input field set to '100'.
- Font Color:** A color selection box showing white.
- Font Size:** A dropdown menu set to '12'.
- Includes:** Three checked checkboxes for 'Username', 'IP Address', and 'Date'.

3. Click the **Save** button.

When viewing the content in the browser, your watermarks appear depending on your chosen settings. Sample watermark options are shown in the following images.

Note

- The message text is forced to one line. Therefore, if your message text is too long, the chosen font size may not be used.
- The watermark is not embedded in the content. Therefore, if a watermark is defined for a source, it is not reflected in the session that uses that source or a video recording from that source.

[Top Left](#) [Center](#) [Center Diagonal](#) [Bottom Right](#)

This watermark shows green text, IP address, username, and date in the top left of the video.



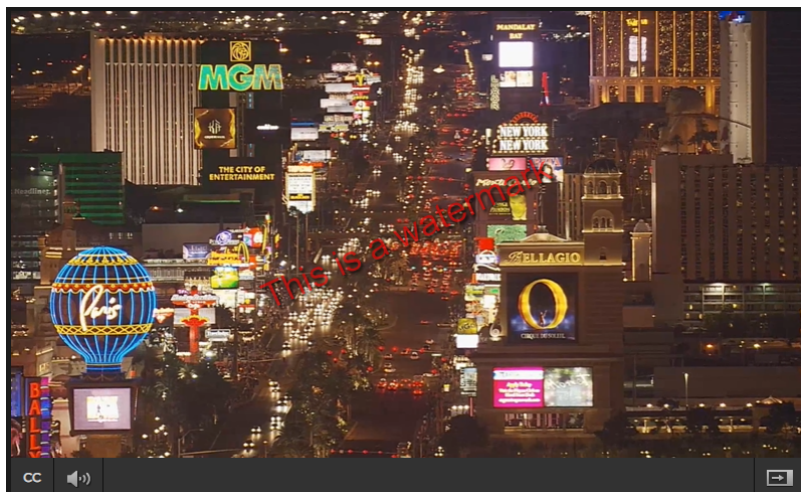
[Top Left](#) [Center](#) [Center Diagonal](#) [Bottom Right](#)

This watermark shows green text, IP address, username, and date in the center of the video with 50% transparency.



[Top Left](#) [Center](#) [Center Diagonal](#) [Bottom Right](#)

This watermark shows red text in the center of the video with 70% transparency and rotated diagonally.



[Top Left](#) [Center](#) [Center Diagonal](#) [Bottom Right](#)

This watermark shows red text and date in the bottom right of the video with 70% transparency.



Source Settings




The following table lists the Source configuration settings:

[Information](#) [SRT Settings](#) [RTMP Settings](#) [RTSP Settings](#) [Metadata](#) [Advanced](#)


Setting	Default	Description/Values
ID	—	HMP assigns a unique identifier (ID) to each source when it is defined. <div style="border: 1px solid #ccc; padding: 5px;"> <p>⚠ Note</p> <p>If you are using the HMP Command Line API, you need to copy this ID to add this source to a session.</p> </div>
Name	Date, time	Enter a name for the source. This name is selectable on the Sources list when content creators define sessions.
Description	—	Enter a description for the source.
Receiver	Current HMP server	To associate the source with a Media Gateway receiver for multi-site live distribution, select a defined Media Gateway from the list (see Configuring Multi-Site Live Distribution).
Type	UDP	Select the protocol type: <ul style="list-style-type: none"> • UDP • SRT (see the SRT Settings section of this table) • RTMP (see the RTMP Settings section of this table) • RTSP (see the RTSP Settings section of this table) <div style="border: 1px solid #ccc; padding: 5px;"> <p>⚠ Note</p> <p>RTMP and RTSP are available only in multi-site live configurations when Media Gateway is selected in the Receiver dropdown.</p> </div>
Address	—	Type in the IP address for the source.
Port	—	Type in the port number for the source.
Multicast Stream	Enabled	(UDP only) Indicates this is a multicast stream.
View Direct	Disabled	(UDP only) Specifies that the Haivision Play Set-Top Box uses the configured Source URL directly and not an HLS version of the stream. If a multicast source has View Direct enabled, the Web player starts the Multicast Agent to receive the source directly on the client and flip to the browser. If the source is embedded in a session or does not have View Direct enabled, the video flows through the normal multi-site live distribution mechanism (which requires at least one Media Gateway).
Low Latency	Disabled	(Available with Live Review license only) Enable the low latency player for the source. <div style="border: 1px solid #ccc; padding: 5px;"> <p>⚠ Note</p> <ul style="list-style-type: none"> • Low latency is currently in Preview Mode. • Low latency distribution of a unicast stream from HMP uses additional system resources. Only enable this feature for streams with very limited viewership or streams that are always distributed to clients via multicast. • Closed captions are not supported by the low latency player. </div>
IPTV Channel	Disabled	Specifies that the source is used in IPTV workflows. It is added to the IPTV Channels list (see Configuring IPTV Channels), as well as in the Program Guide on Haivision Play Set-Top Boxes. You can configure IPTV channels and assign access from here or from the IPTV Channels pane.

Setting	Default	Description/Values
Channel Number	Highest channel number + 1	Specifies the channel number used in the IPTV Channels list and in the Program Guide. Range = 1-9999.
EPG	Off	To enable EPG display on set-top boxes, toggle the EPG button to On. (EPG must be licensed on your system.)
Schedule	First channel on list	(EPG must be On) Select the schedule for the EPG display from the drop-down list.

Information SRT Settings RTMP Settings RTSP Settings Metadata Advanced

Setting	Default	Description/Values
Mode	Caller	<p>Specifies the SRT Connection Mode:</p> <ul style="list-style-type: none"> • Caller: HMP acts like a client and connects to a server listening and waiting for an incoming call. • Listener: HMP acts like a server and listens/waits for clients to connect to it. • Rendezvous: Allows calling and listening at the same time. <div style="border: 1px solid #c6e0b4; padding: 5px; margin-top: 10px;"> <p> Tip To simplify firewall traversal, Rendezvous Mode allows HMP and the encoder to traverse a firewall without the need to open a network port</p> </div> <div style="border: 1px solid #fff9c4; padding: 5px; margin-top: 10px;"> <p> Note See Configuring Secure Reliable Transport (SRT) Sources.</p> </div>
Latency	125 ms	<p>Specifies how long HMP buffers received packets. The size of this buffer adds up to the total latency. A minimum value must be 3 times the round-trip-time (RTT). Range = 20-8000 ms</p> <div style="border: 1px solid #fff9c4; padding: 5px; margin-top: 10px;"> <p> Note Latency is for the SRT protocol only and does not include the capture, encoding, decoding and display processes of the endpoint devices.</p> </div>
Passphrase	—	<p>(Optional, must match encoder passphrase) This parameter is required if the stream is encrypted and is used to retrieve the cryptographic key protecting the stream. Range = 10-79 UTF-8 characters</p>

Information SRT Settings RTMP Settings RTSP Settings Metadata Advanced

 **Note**

Only available in multi-site live configurations when a Media Gateway is selected in the Receiver dropdown.

Setting	Description/Values
Stream Name	Desired name for the source stream.
Mode	Select the mode for connection to the RTMP stream: <ul style="list-style-type: none"> • Publisher: Stream sent directly to the Media Gateway's IP address. For more details regarding RTMP Publisher mode see Example: Connecting an RTMP Publisher Source in the <i>Haivision Media Gateway User's Guide</i>. • Consumer: Stream available for Media Gateway to access on an RTMP server.

Information SRT Settings RTMP Settings RTSP Settings Metadata Advanced

Note

Only available in multi-site live configurations when a Media Gateway is selected in the Receiver dropdown.

Setting	Description/Values
RTSP Username/Password	The username and password for the RTSP stream.

Information SRT Settings RTMP Settings RTSP Settings Metadata Advanced

Setting	Default	Description/Values
Metadata	—	(Optional) To assign metadata to the source, select a key and select one or more values or (where allowed) type in custom values <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>Metadata keys and values must be pre-defined on your system. See Defining Metadata.</p> </div>

Information SRT Settings RTMP Settings RTSP Settings Metadata Advanced

Setting	Default	Description/Values
Player Tuning		
Profile	Default	(For advanced users only) To change the STB player tuning profile used by the source, select the desired profile from the drop-down list. See Adjusting STB Player Tuning for defining the available tuning profiles.
Watermarking		
Active	Off	Toggle to enable/disable watermarking for the source
Message	—	Message to display on the watermark.
Anchor	Top Left	Location to place the watermark on the video source: Top Left, Top Right, Center, Bottom Left, or Bottom Right.

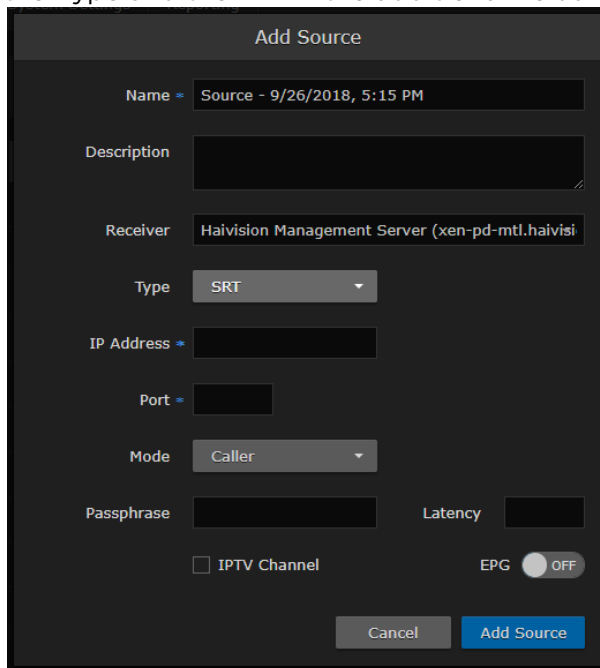
Orientation	Horizontal	Orientation of the text on the video source: Horizontal or Diagonal.
Transparency	100%	Transparency of the watermark on the video source in percent. Range: 0-100.
Font Color	White	Font color of the watermark.
Font Size	12	Font size of the watermark.
Includes	All enabled	Checkboxes to enable/disable the display of user- and time-specific data in the watermark: Username, IP Address, and Date.

Configuring Secure Reliable Transport (SRT) Sources

Haivision’s Secure Reliable Transport (SRT) streaming protocol is designed to provide reliable and secure end-to-end transport between two SRT-enabled devices (such as a Makito X encoder or Media Gateway and Haivision Media Platform) over a link which traverses the public Internet. SRT optimizes video streaming performance across unpredictable Internet networks, recovering from packet loss, jitter, network congestion and bandwidth fluctuations that can severely affect the viewing experience.

To create an SRT connection:

1. Ensure the encoder or Media Gateway and HMP are accessible from the public Internet by appropriate configuration of any firewalls.
2. Create an HMP source using the SRT streaming protocol. On the Add Source dialog, select SRT for the Type and then fill in the additional fields. For details, see "SRT Settings" under [Source Settings](#).




3. Set up the SRT stream on the encoder or Media Gateway and start the stream connection.
4. Using the statistics page on your Media Gateway, monitor the link statistics to see if the link is oversubscribed (and if it is, adjust the video encoder bitrate).

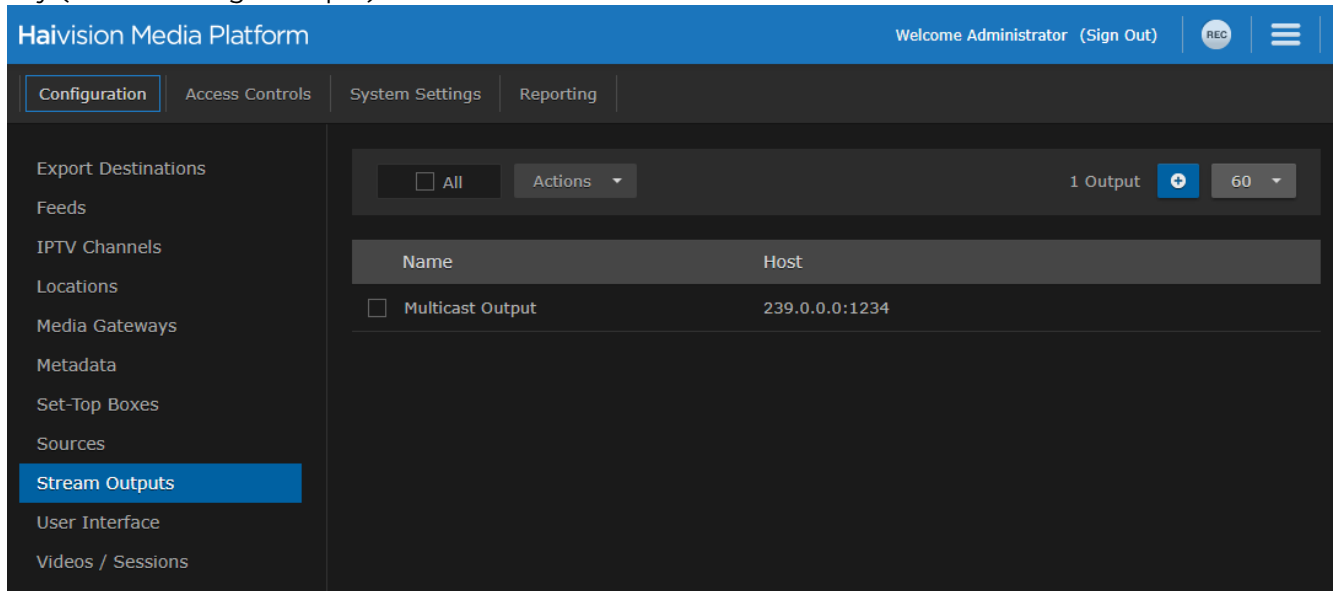
For additional information required to configure and tune SRT streams, please see the [SRT Deployment Guide](#).

Managing Stream Outputs


When setting up Haivision Media Platform, you can define multiple stream outputs for users to select from when re-streaming videos. (They can also specify an IP address and port for the streaming output.) With multi-source videos, users can choose the track to re-stream and then choose a different streaming output for each track. See [Re-Streaming Videos](#) in the User’s Guide.

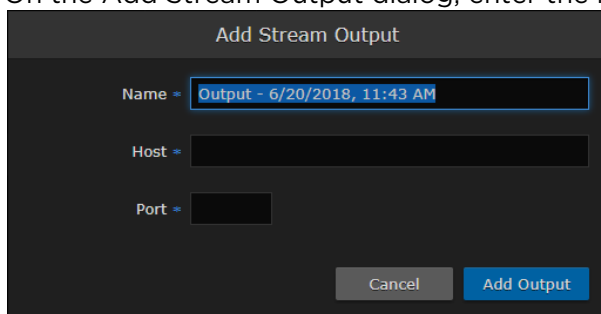
To manage stream outputs:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **Stream Outputs** on the sidebar. The Stream Outputs pane opens, displaying the list of defined stream outputs for your system, if any (see following example).



To add a stream output:

1. From the Stream Outputs pane, click the  icon.
2. On the Add Stream Output dialog, enter the name, host IP address or URL, and port for the output.



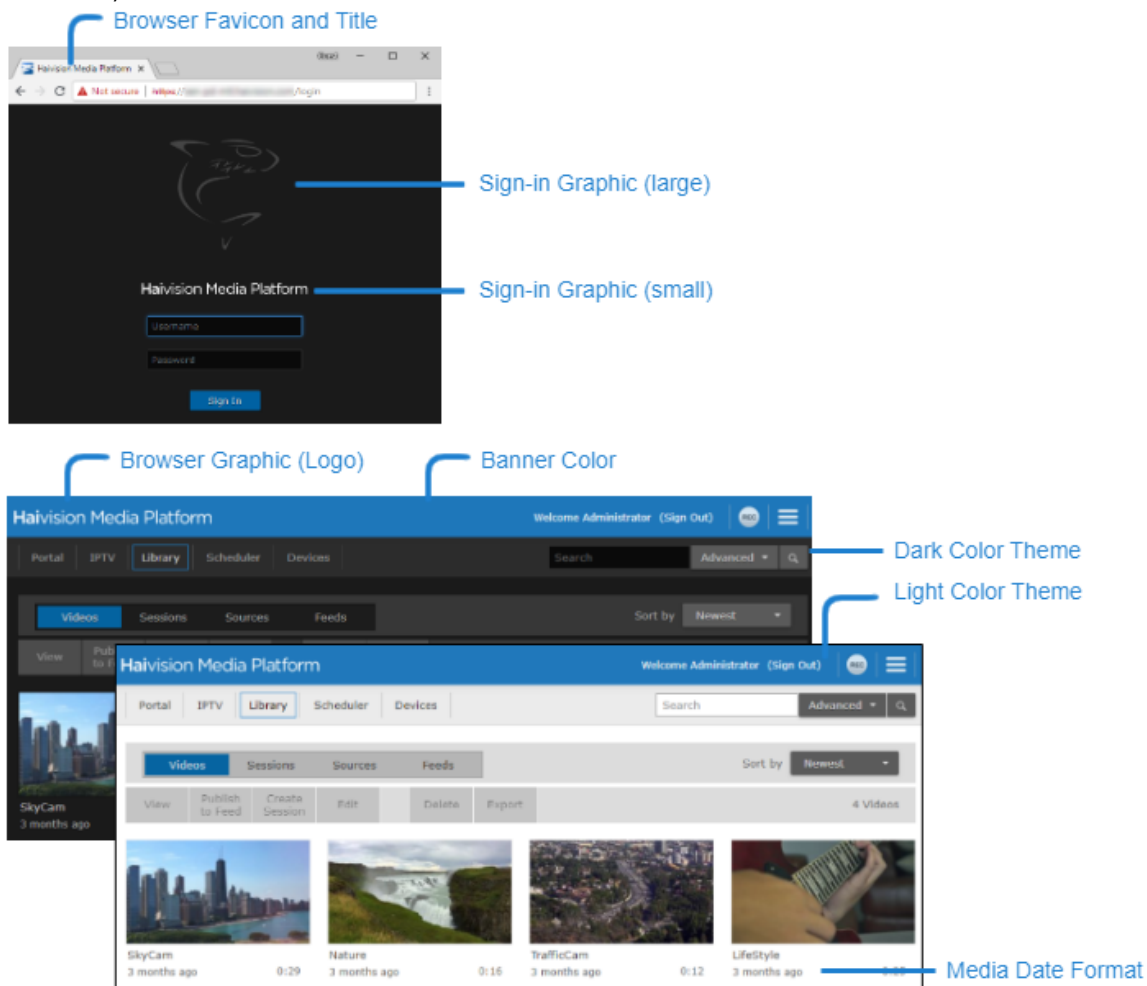
3. Click **Add Output**. The new output is added to the Stream Outputs list.

Re-Branding the User Interface


From the User Interface page, you can customize the Haivision Media Platform user interface to suit your organization. For example, you can add your own branding images and color (which are applied to all users the next time the user's browser window is refreshed). You can also disable the display of one or both Sign-In page graphics.

You can customize the following user interface components:


- The favicon and title that browsers display in tabs and bookmarks
- The logos that appear on the sign-in page
- The banner graphic (logo) at the top left of the interface
- The color of the top banner
- The color scheme: dark or light
- The date/time format for videos and sessions



To customize the HMP user interface:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **User Interface** on the sidebar.
3. The User Interface pane opens allowing you to change various aspects of the user interface. See [User Interface Settings](#) for each option.

 **Tip**

- To view additional help for a setting, hover the cursor over the  icon.
- To revert to the default image or banner color, click **Reset**.

4. Click **Save Settings**.


Related Topics

- [User Interface Settings](#)

User Interface Settings

The following table lists the User Interface configuration settings: (For corresponding illustrations, see [Re-Branding the User Interface](#).)

[Display Settings](#) Branding Mobile Branding

Setting	Default	Description/Values
Media Date Format	Human Friendly	Configures the display of date and time for videos and sessions in the browser and devices. <ul style="list-style-type: none"> • Human Friendly (default). For example, "21 days ago". • Timestamp. For example, "12/13/2019, 9:42 PM". • Timestamp 24hr. For example, "12/13/2019, 21:42:43". <div style="border: 1px solid #ffc107; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>When changing the media date format:</p> <ul style="list-style-type: none"> • Play 1000 STBs require a reboot for the change to take effect. • Play 2000 and 4000 STBs require either a toggle of the STB Settings screen or a reboot for the change to take effect. </div>

[Display Settings](#) [Branding](#) Mobile Branding

Setting	Default	Description/Values
Color Scheme	Dark	Switch interface between dark and light color schemes. <ul style="list-style-type: none"> • Dark: black background with white text (default) • Light: white background with black text.
Banner Color	Haivision blue (RGB: 27-117-188)	The color of the banner along the top of the page.

Setting	Default	Description/Values
Banner Graphic	Haivision Media Platform text logo (235x16px PNG)	The image/logo on the left side of the banner. The width of the image can be as long as needed up to a recommended maximum of 300 x 47 pixels. However, it should not run into the username (on the right side of the banner). Also, keep in mind that this is affected by factors such as window size, browser, etc.
Sign-in Graphic (large)	Haivision shark logo	The top image on the Sign-in page. The width and height can be any dimension up to a recommended maximum of 4000 x 4000 pixels. <div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>⚠ Note You can use this setting to create a fullscreen image. However, large images can slow down or prevent page load. Also, if the screen resolution is smaller than the image, the image is cropped. The image is centered horizontally.</p> </div>
Sign-in Graphic (small)	Haivision Media Platform text logo (235x16px PNG)	The lower image on the Sign-in page. The width and height can be any dimension to fit the page. However, the image is resized to 220 pixels wide (while maintaining the aspect ratio). Also, a resized height greater than 400 pixels may require the user to scroll. The image is centered horizontally on the page.
Browser Favicon	Haivision favicon	The image to display in the browser's address bar. <div style="border: 1px solid #ccc; padding: 5px; background-color: #e8f5e9;"> <p>✔ Tip The width and height can be 16, 32, 48, or 64 pixels (squared), 8-bit or 24-bit.</p> </div>
Browser Title	Haivision Media Platform	The text to display in a browser tab/window. Also, used as the name of this HMP system in the Haivision Play for Mobile app.

Display Settings Branding Mobile Branding


✔ Tip
Mobile Branding settings can also be set locally from the Haivision Play for Mobile app.

Setting	Default	Description/Values
System Icon	Haivision mobile system icon	Used to identify the HMP system by icon on a Play Mobile device. <div style="border: 1px solid #ccc; padding: 5px; background-color: #e8f5e9;"> <p>✔ Tip The width and height should be a 132px square (maximum 512 px).</p> </div>

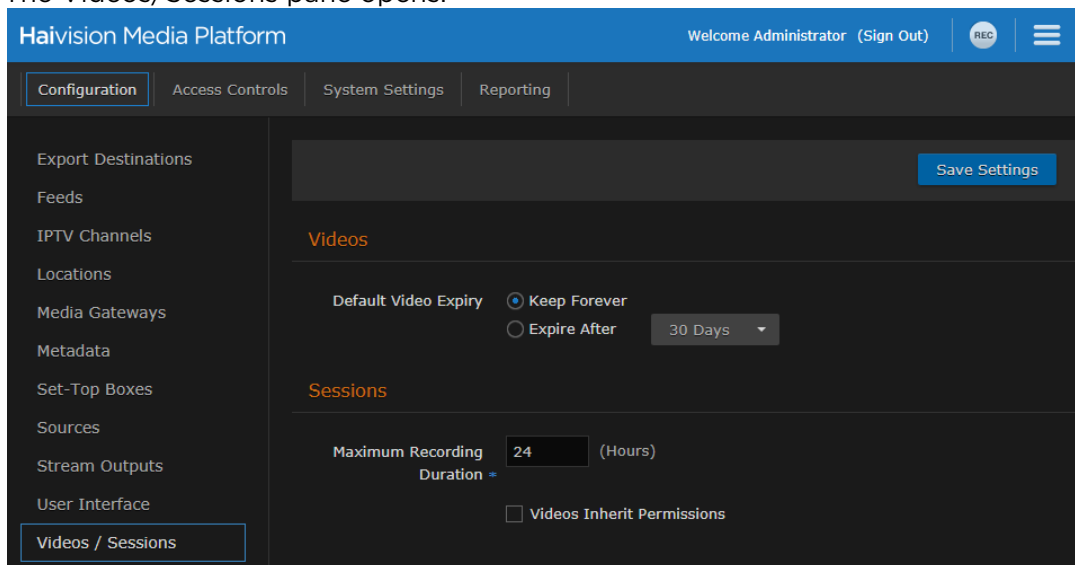
Configuring Video and Session Settings

When setting up Haivision Media Platform, administrators can configure system-wide video and session settings, such as the default video expiry and maximum recording duration.

To configure the video and session settings:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Configuration** on the toolbar and then click **Videos/Sessions** on the sidebar.

The Videos/Sessions pane opens:



- The Default Video Expiry specifies whether videos are kept forever or if they expire and are deleted after a specified number of days. Setting a global timer to delete videos saves you from having to spend time cleaning up old videos.

 **Note**

Modifying a video does not reset the timer; it is based on the creation time. Trimming a video creates a new video and resets the timer for that new video, but leaves the old one unchanged.

Users can override the Default Video Expiry on a per-video basis. For details, see [Editing Video Information and Metadata](#) in the User’s Guide.

- For the Maximum Recording Duration, type in the maximum number of hours. HMP stops recording when reaching that duration.
- To allow a session’s sharing permissions to be passed to videos made from that session (disabled by default), check the Videos Inherit Permissions checkbox. The objective is a workflow decision to help reduce the number of times a user must enter the sharing dialog. Permissions are copied at the start of the recording. The recording creator is still granted "OWN" permissions on the new video.


3. Click **Save Settings**.

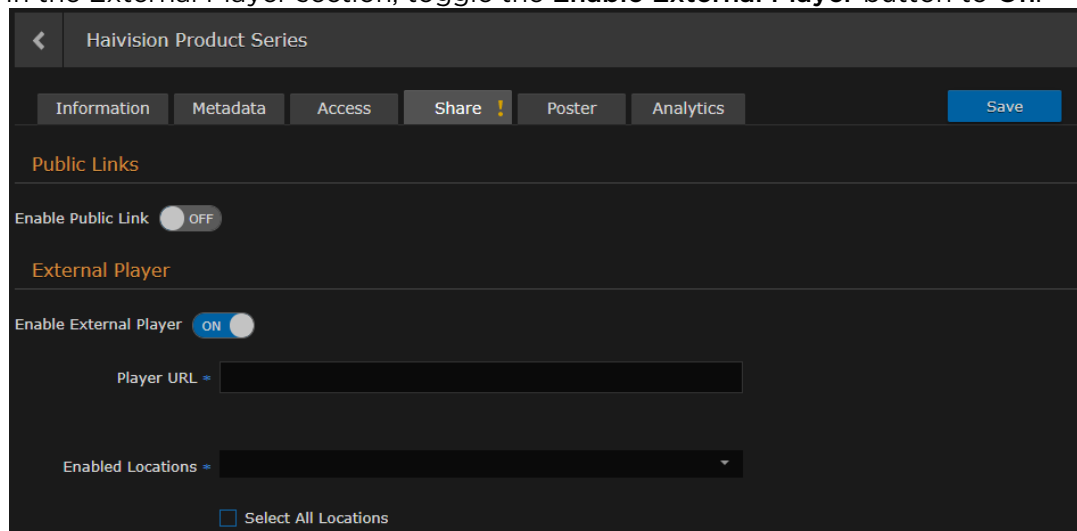
Using an External Player to View Sessions

Instead of users viewing sessions with the built-in HMP player, as an administrator you can specify an external video player (e.g. the Microsoft Stream player) to help the HMP system reach large-scale internet

audiences for live event streaming. You may also specify the viewer locations which should use the external player. All other locations use the HMP player.

To enable an external player for a session:


1. On the Sessions list click  icon on the session you want to edit to open the Information pane.
2. Click the **Share** tab.
3. In the External Player section, toggle the **Enable External Player** button to **On**.



4. In the Player URL text box, enter the URL for the external player.
5. In the Enabled Locations dropdown, select which locations will use the external player.

Tip

- If you defined a default location in [Configuring Locations](#), it is automatically added to the Enabled Locations list.
- If you start typing in the text box, HMP displays a drop-down list of matching values that you can choose from.

6. To enable the external player for all locations, check the Select All Locations checkbox. All locations are added to the Enabled Locations text box.
7. Click the **Save** button.
8. To return to the Library's Sessions list, click the  icon.


Adjusting STB Player Tuning

Caution

For advanced users only. Changing the STB tuning configuration impacts the reliability of video playback. Please contact [Haivision Support](#) for guidance prior to using this feature.

STB tuning profiles may be selected for each source as shown in [Source Settings](#).

To view the current tuning profiles:

1. Click the  icon and select **Administration**.
2. Click **Configuration** and click **Player Tuning**.
3. Click file link next to Current Tuning Profiles.
The current tuning profile JSON file is downloaded by your browser.

To adjust the available tuning profiles for your sources:

1. On the **Player Tuning** screen, drag a tuning configuration file to the drop area or click **Choose a file** and select the file.

 **Note**

The tuning configuration file must be valide JSON.

2. Click the **Upload** button.
The new tuning profiles are now used for each source.

To reset the tuning profiles to default:

1. On the **Player Tuning** screen, click the **Reset All** button.
2. Confirm your action in the confirmation dialog.
The default tuning profiles are now used for each source.

Managing Access Controls

This section describes how to set up and manage user accounts, groups, roles, and access permissions for your Haivision Media Platform (HMP).

Important

Before proceeding, ensure that sources and (if applicable) Directory Authentication Services have been configured for your system. See [Managing Sources](#) and [Managing Directory \(Authentication\) Services](#).

Topics Discussed

- [Managing Users](#)
 - [Assigning Roles to LDAP/AD Users](#)
 - [Managing User Accounts \(Non LDAP/AD\)](#)
 - [User Settings](#)
- [Managing Groups \(LDAP/AD Only\)](#)
 - [Assigning Roles to LDAP/AD Groups](#)
- [Managing Roles](#)
 - [Adding Users and Groups to Roles](#)
 - [Editing Role Permissions](#)
 - [Creating Custom Roles](#)
 - [Default Roles](#)
 - [Customizing the Navigation Toolbar for Each Role](#)
- [Managing Access Permissions](#)

Managing Users

Important

If HMP is connected to an LDAP or Active Directory server, the Users list is populated with information from the directory server. See [Assigning Roles to LDAP/AD Users](#).


Haivision Media Platform allows you to display a list of users and assign roles to users. HMP uses roles with pre-defined permissions to provide users or groups with controlled access to videos, sessions, and sources. To successfully sign in, a user must be assigned a role.

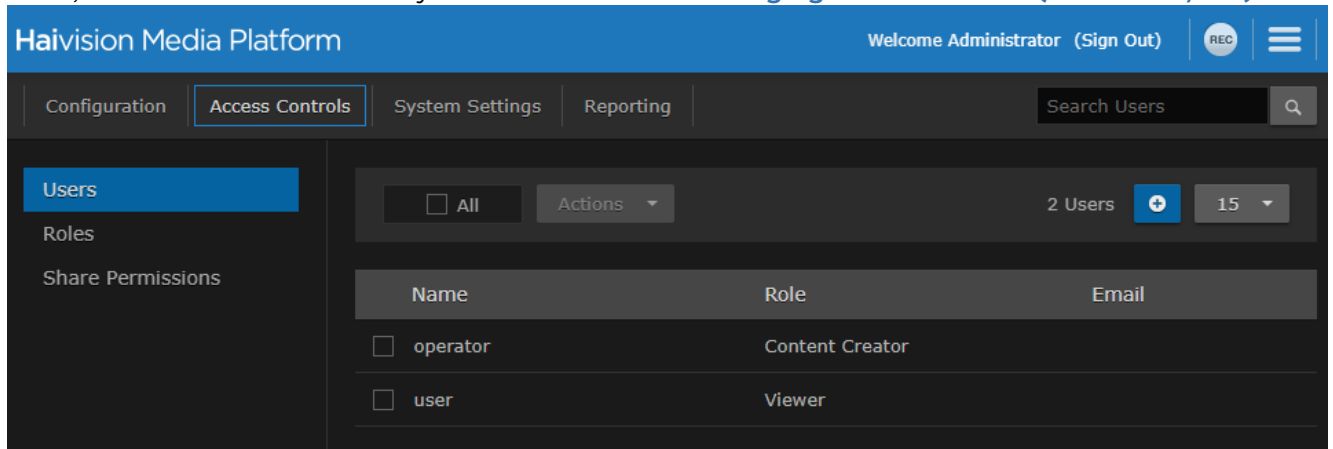
If your system is *not* connected to a directory server, you may also add and modify user accounts from HMP.

Note

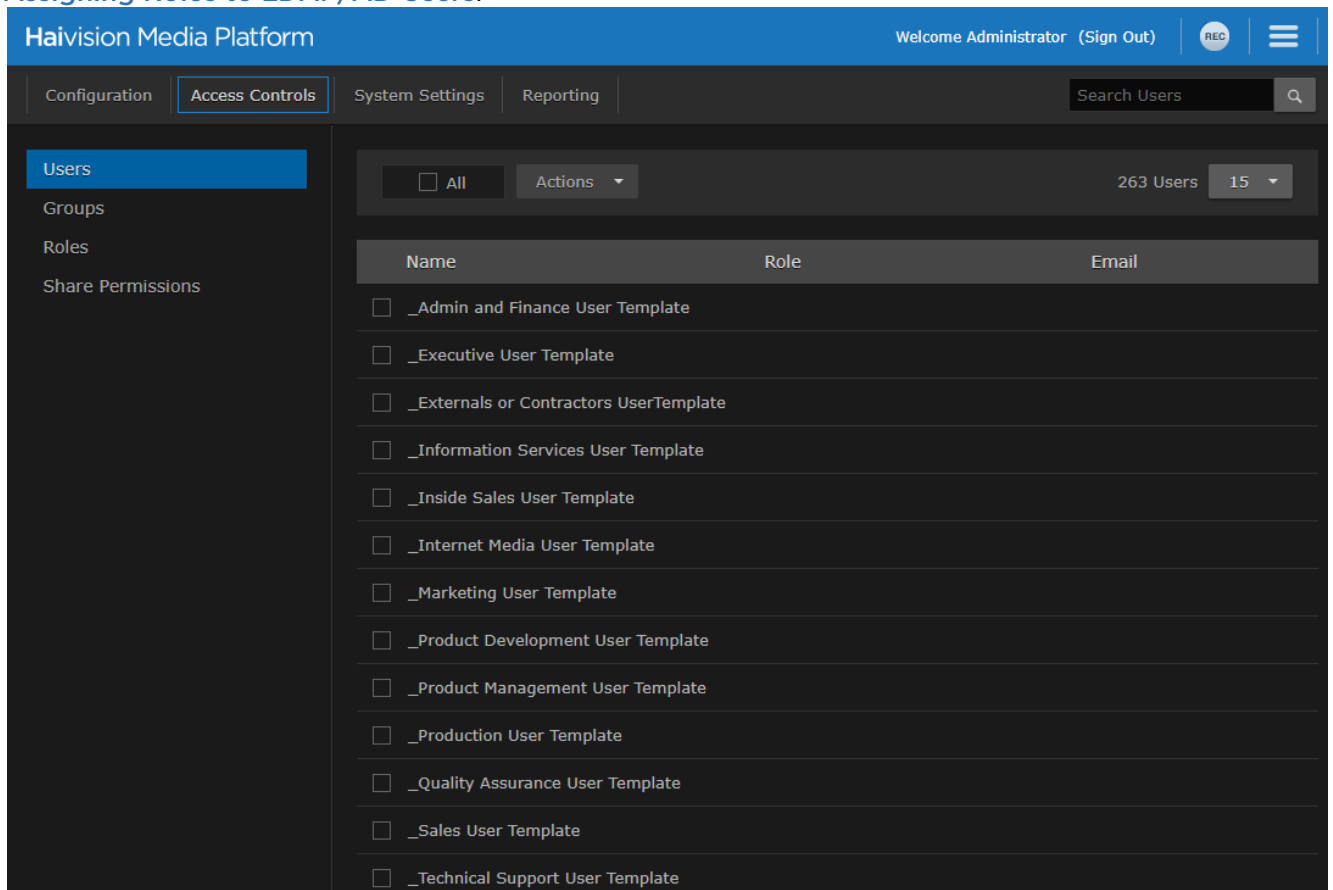
Although the typical workflow in an LDAP/AD environment is to assign roles via Groups, assigning roles from the Users list may be useful in some cases.

To view and manage the users for your platform:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Access Controls** on the toolbar and then click **Users** on the sidebar.
The Users list opens, displaying the list of defined users for your platform.
3. If HMP is not connected to a directory server, you may browse through the list, assign roles to users, as well as add and modify user accounts. See [Managing User Accounts \(Non LDAP/AD\)](#).



In an LDAP/AD environment, you may browse through the list and assign roles to users. See [Assigning Roles to LDAP/AD Users](#).



Topics Discussed

- [Assigning Roles to LDAP/AD Users](#)
- [Managing User Accounts \(Non LDAP/AD\)](#)
- [User Settings](#)

Assigning Roles to LDAP/AD Users

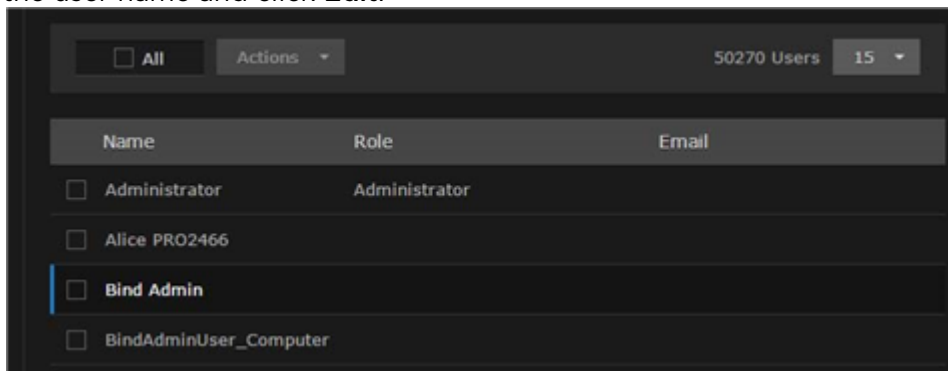
⚠ Important

If HMP is connected to a directory server, user accounts must be created or modified from the LDAP or Active Directory server. You cannot add or modify user accounts from HMP. HMP users will sign in using their LDAP/AD username and password.

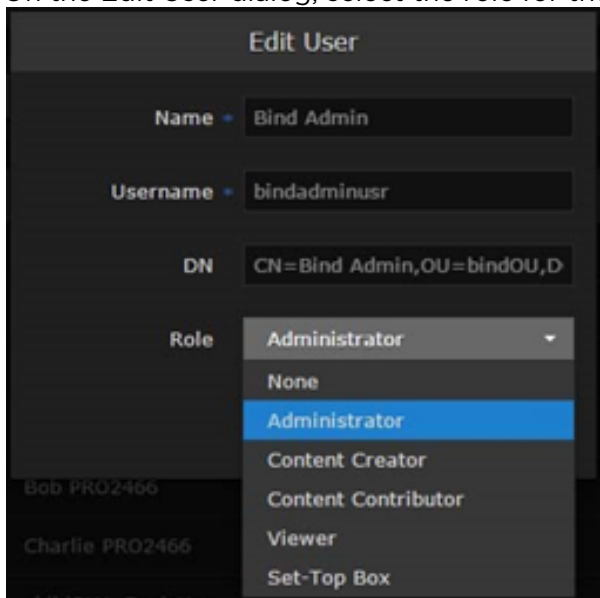
In an LDAP/AD environment, you may browse through the Users list and assign roles to users.

To assign a role to a user:

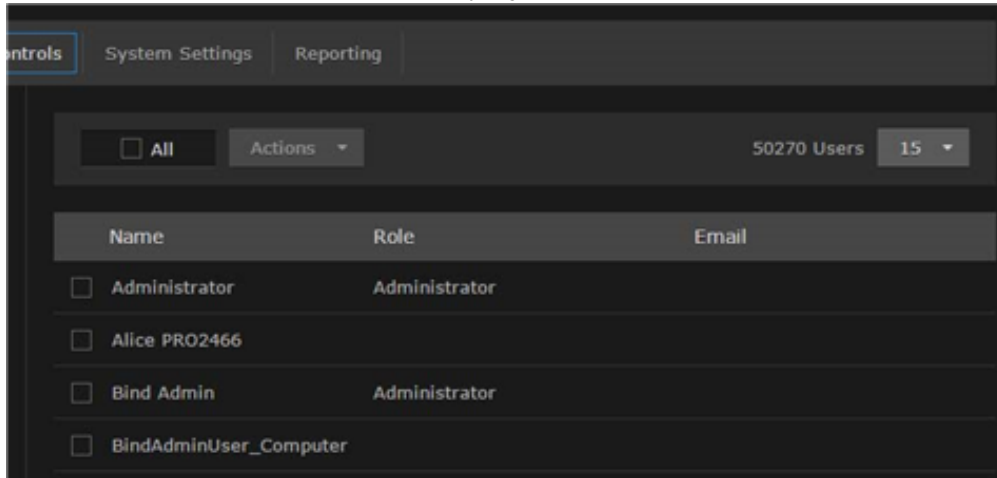
1. Select the user by clicking the user name in the Users list, or you can check the checkbox next to the user name and click **Edit**.



2. On the Edit User dialog, select the role for the user account. See the Role entry in [User Settings](#).



3. Click **Save User**. The new role is displayed on the Users list.



Related Topics

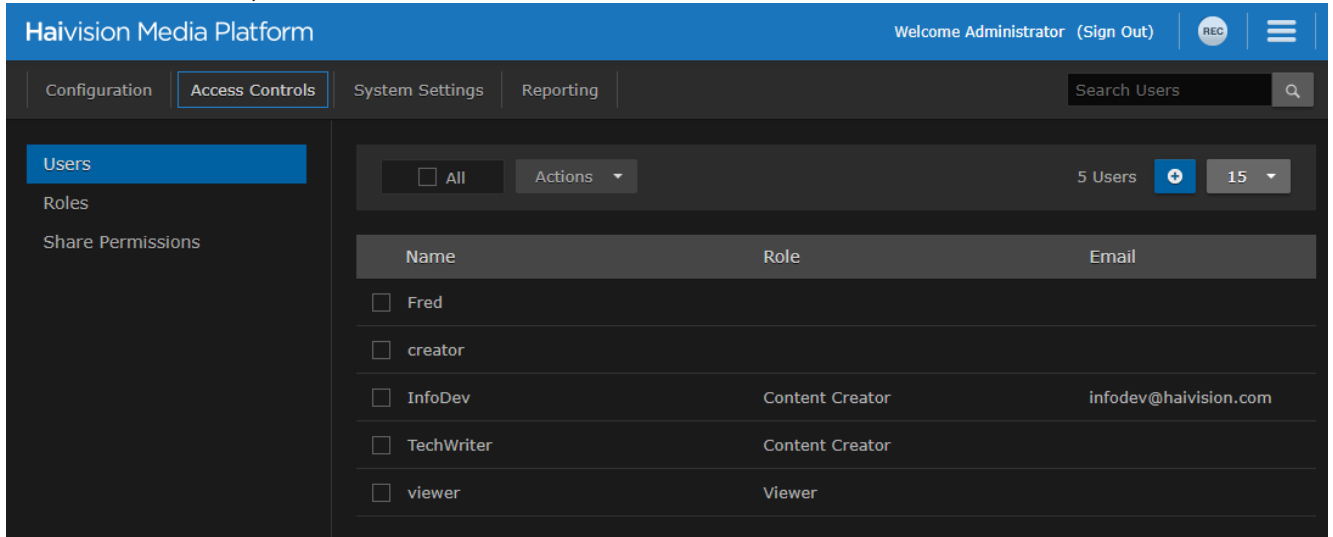
- [User Settings](#)

Managing User Accounts (Non LDAP/AD)

If HMP is *not* connected to a directory server, you need to add and modify user accounts from the Users list.

To add a user:

1. From the Users list, click the **+** icon.



2. On the Add User Information dialog, enter or select the value(s) to define the user. See [User Settings](#).

3. Click **Add User**. The new user is added to the Users list.

Related Topics

- [User Settings](#)

User Settings

The following table lists the configurable User settings on non-LDAP/AD systems:

User Setting	Default	Description/Values
Name	—	Enter a name for the user. This name is displayed on the Users list.
Username	—	Enter a unique username. The user uses this name to sign into the HMP Web interface. <div style="border: 1px solid #ffc107; padding: 5px; margin-top: 10px;">⚠ Note You cannot modify the username.</div>
Password	—	Type in the new password.
Confirm Password	—	Type in the new password again.
Email	—	Enter an email address to associate with the user account.

User Setting	Default	Description/Values
Role	None	<p>Select the role for user. To successfully sign in, a user must be assigned a role (other than none).</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>⚠ Note</p> <p>For information on creating and customizing roles for your system, see Managing Roles. For the default role permissions, see Default Roles.</p> </div>


Managing Groups (LDAP/AD Only)

⚠ Important

Groups are only available on Haivision Media Platform if your system is connected to an LDAP or Active Directory server. See [Managing Directory \(Authentication\) Services](#).

If Haivision Media Platform is connected to an LDAP or Active Directory server, the Groups list is populated with information from the directory server. From the Groups list, you can assign roles to groups. This provides a means to efficiently manage multiple users. You cannot add or modify groups directly from HMP.

To view and manage the groups for your platform:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Access Controls** on the toolbar and then click **Groups** on the sidebar.
The Groups list opens, displaying the list of defined groups for your platform (shown in the

following example, connected to an Active Directory server).

The screenshot shows the 'Access Controls' section of the Haivision Media Platform. The left sidebar contains navigation options: Users, Groups (selected), Roles, and Share Permissions. The main content area displays a table of groups with checkboxes for selection. The table has columns for 'Name' and 'Role'. The 'Edit' button is visible at the top right of the table area, along with a count of '214 Groups' and a dropdown menu showing '15'.

Name	Role
<input type="checkbox"/> APTTESTusers	
<input type="checkbox"/> Accpac	
<input type="checkbox"/> Admin and Finance	
<input type="checkbox"/> Admin and Finance - RO	
<input type="checkbox"/> Admin and Finance - RW	
<input type="checkbox"/> All Employees	
<input type="checkbox"/> Allowed RODC Password Replication Gro...	
<input type="checkbox"/> BacklogAdmins	
<input type="checkbox"/> BackupStorage	
<input type="checkbox"/> CAED	
<input type="checkbox"/> Cert Publishers	
<input type="checkbox"/> Checklist_Admin	

3. To assign roles to groups, see [Assigning Roles to LDAP/AD Groups](#).

Assigning Roles to LDAP/AD Groups

⚠ Important

- If Haivision Media Platform is connected to an LDAP or Active Directory server, the HMP Groups list is populated with information from the directory server. See [Managing Directory \(Authentication\) Services](#).
- Groups must be created or modified from the directory server. You cannot add or modify groups from the HMP Web interface, other than to assign the role.

To assign a role to a group:

1. Select the group name in the Groups list.
2. On the Group Information dialog, select the role for the group. See [Default Roles](#).

3. Click **Save Group**. The new role is displayed on the Groups list.

Name	Role
<input type="checkbox"/> APTESTusers	
<input type="checkbox"/> Accpac	
<input type="checkbox"/> Admin and Finance	Content Creator
<input type="checkbox"/> Admin and Finance - RO	
<input type="checkbox"/> Admin and Finance - RW	

Managing Roles

Roles are used to confer permissions to users and groups. A user must be assigned a role to sign in. Haivision Media Platform provides the following default roles.

Role	Default Permissions
Administrator	In charge of system.
Content Creator	Make sessions, record videos, and manage feeds; no control over sources.
Content Contributor	Record videos with no other system responsibilities.
Viewer	View or interact with content with no other system responsibilities.
Set-Top Box	Same as Content Creator with Set-Top Box administration added.

 **Note**

For more information, see [Default Roles](#).

In addition, users may be assigned access permissions for content rights (videos, sessions, and sources) by administrators or other users. Access permissions may further qualify a user's privileges. HMP roles and access permissions are fully customizable (see [Creating Custom Roles](#) and [Managing Access Permissions](#)). When a user belongs to a group, the user's permissions are a combination of both.

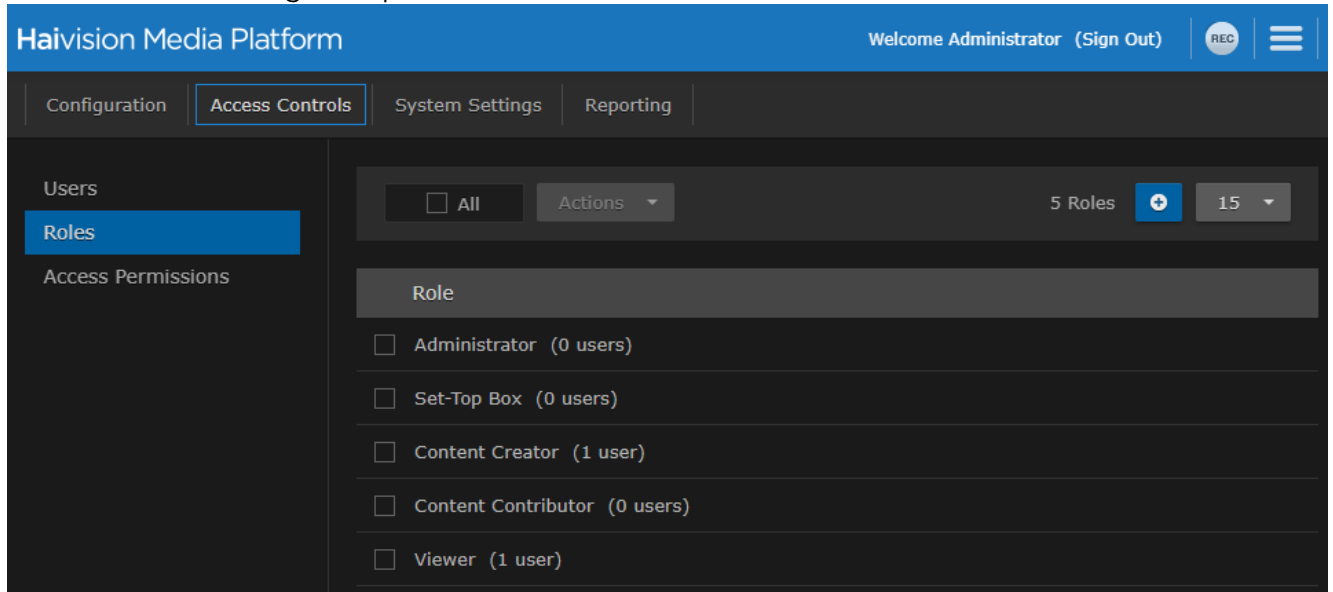
 **Tip**

The best practice is to assign a lower role to the group, and then assign higher roles to individual users as required.

To view and manage the roles for your platform:

1. Click the  icon and select **Administration** from the navigation drop-down menu.

- Click **Access Controls** on the toolbar and then click **Roles** on the sidebar. The Roles list opens, as shown in the following example.



The Roles list displays the list of available roles and the number of users (and groups, if applicable) assigned to each role. From here, you can add users to and remove users from an existing role, and edit role permissions. You can also create new roles and delete roles.

- To add users (and groups, if applicable) to a role, see [Adding Users and Groups to Roles](#).
- To edit role permissions, click the role to edit. See [Editing Role Permissions](#) for more details.
- To create a new role, click the **+** button. See [Creating Custom Roles](#) for more details.
- To delete roles, select one or more roles and click **Actions > Delete**.

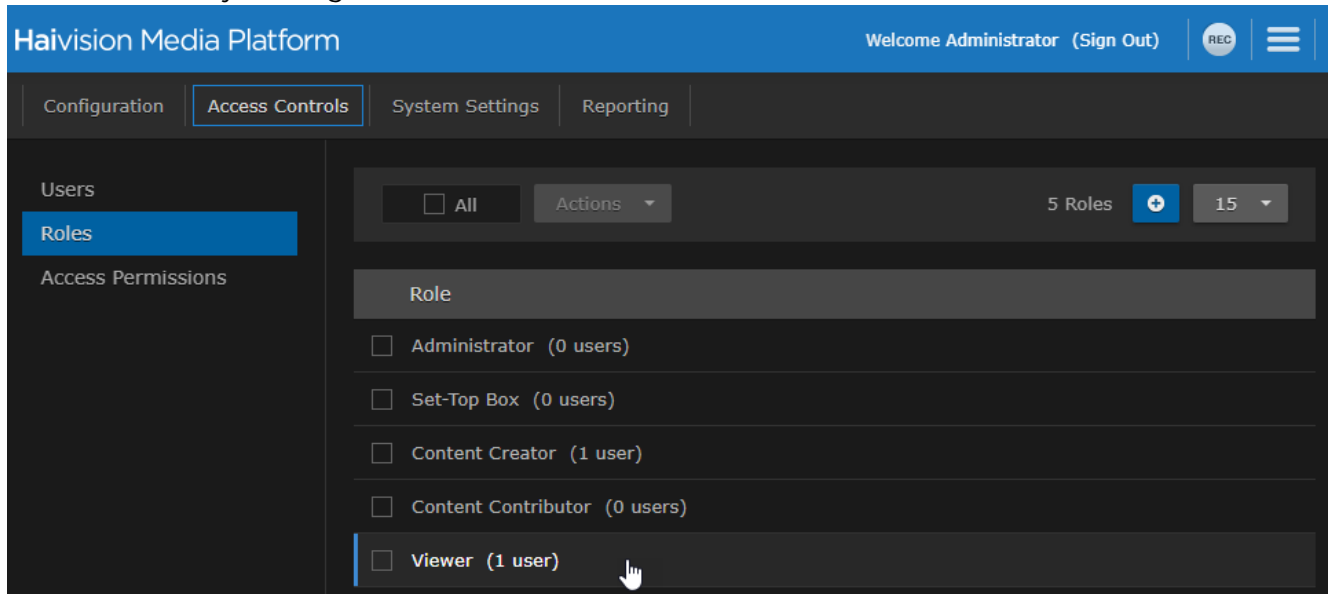
Related Topics

- [Default Roles](#)

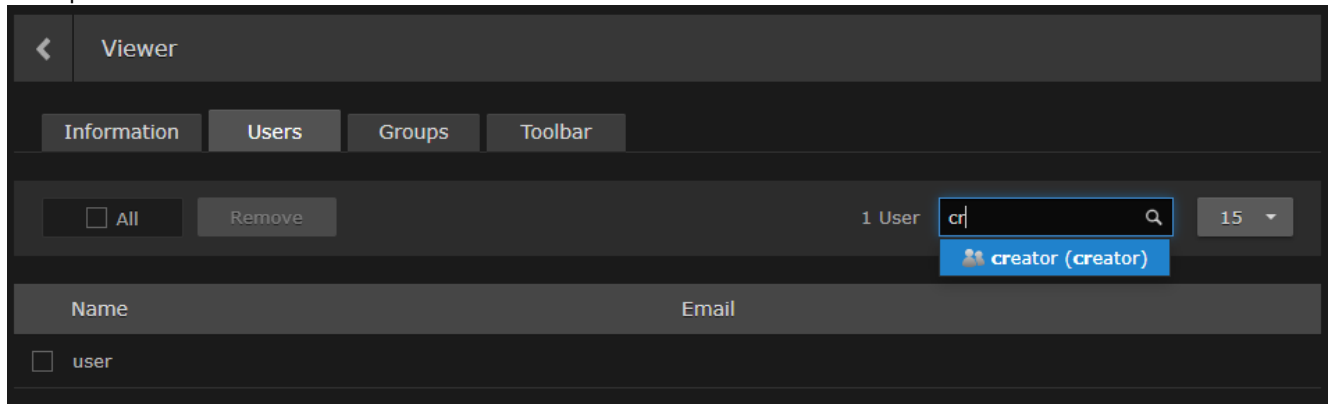
Adding Users and Groups to Roles


To add users and/or groups to a role:

1. Select the role by clicking the role name.



2. On the Information pane, click the **Users** or **Groups** tab.
3. On the Users or Groups pane, type the first few letters of the user or group name in the Add User/ Group search field.



4. Select the user or group from the list that appears. The selected user or group is now added to the role.
5. Click the  icon to return to the Roles list.

Editing Role Permissions

To edit permissions for a role:

1. Click the role in the Roles list.

2. On the Information pane, check or uncheck the permissions as required.

The screenshot shows the 'Viewer' role configuration page. At the top, there are tabs for 'Information', 'Users', 'Groups', and 'Toolbar'. A 'Save Role' button is in the top right. The role name is 'Viewer' and 'Administrator Privileges' is turned off. The 'Permissions' section is divided into several categories:

Video	Session	Source	Layout
<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Access Control	<input type="checkbox"/> Access Control	<input type="checkbox"/> Create
<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Change Sources	<input type="checkbox"/> Create	<input type="checkbox"/> Delete
<input checked="" type="checkbox"/> Download	<input checked="" type="checkbox"/> Create	<input type="checkbox"/> Delete	<input type="checkbox"/> Edit
<input checked="" type="checkbox"/> Edit Metadata	<input checked="" type="checkbox"/> Delete	<input type="checkbox"/> Edit Metadata	<input type="checkbox"/> View
<input type="checkbox"/> Export	<input checked="" type="checkbox"/> Edit Metadata	<input checked="" type="checkbox"/> View	Feed
<input type="checkbox"/> Import	<input checked="" type="checkbox"/> Live On/Off		<input type="checkbox"/> Change Content
<input type="checkbox"/> Mobile Offline Viewing	<input checked="" type="checkbox"/> Record		<input checked="" type="checkbox"/> View
<input checked="" type="checkbox"/> Restream	<input checked="" type="checkbox"/> View	Analytics	Administration
<input checked="" type="checkbox"/> Trim		<input type="checkbox"/> View	<input type="checkbox"/> Set-Top Box
<input checked="" type="checkbox"/> View			

Tip

To give a role full administrative privileges, toggle the Administrator Privileges button to **On**.

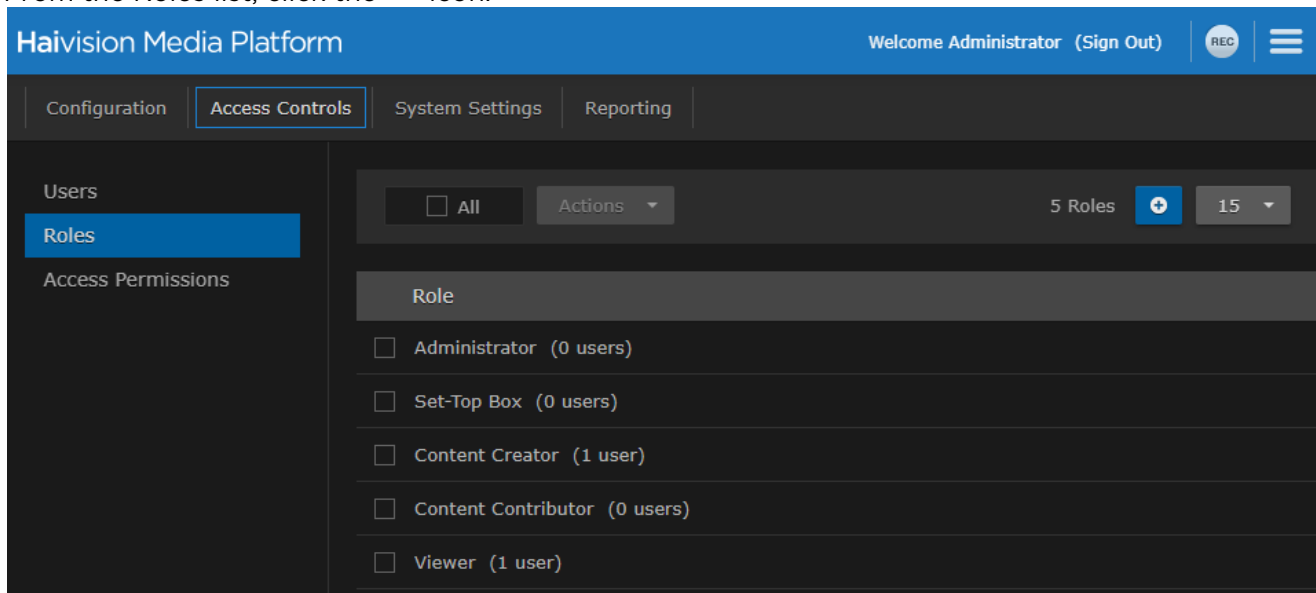
3. Click **Save Role**. The selected permissions are applied to the role.

Creating Custom Roles

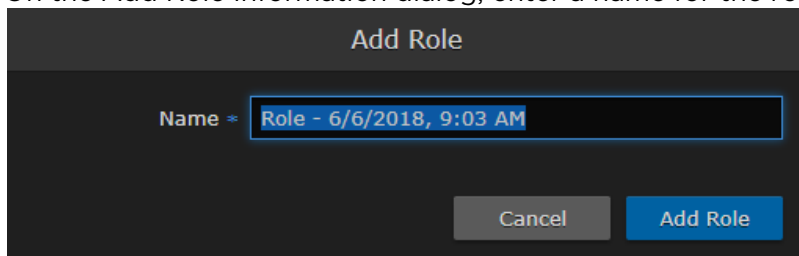
Administrators can create custom roles with full control of fine-grain permissions. For example, end-users can be assigned a role enabling them to create a session but not share it with other users, or to record a video but not download or delete it.

To create a custom role:

1. From the Roles list, click the  icon.




2. On the Add Role Information dialog, enter a name for the role.



3. Click **Add Role**.
4. On the Information pane, check the permissions to assign to the role.

 **Tip**

- View is always enabled for Video, Session, Source, and Feed permissions.
- To give a role full administrative privileges, toggle the **Administrator Privileges** button to **On**.

5. Click **Save Role**.
6. To add users or groups to the role, click **Users** or **Groups** on the sidebar. See [Adding Users and Groups to Roles](#).
7. Click the  icon to return to the Roles list.

Default Roles

The following table is a matrix of the default roles (i.e., for system functions) available to assign to HMP users and groups. In addition, where applicable, the table lists the default access permissions for content rights (videos and sessions).

⚠ Important

- Administrators may create additional roles, as well as edit the permissions for the default roles.
- Role permissions may be further qualified by access permissions. For example, a user with the Viewer role might have been given OWN permissions on a video and can therefore edit and delete it.

[Videos](#) [Sessions](#) [Sources](#) [Layout](#) [Feed](#) [Analytics](#) [Administration](#)

Tasks	Roles				
	Administrator	Content Creator	Content Contributor	Viewer	Set-Top Box
Access Control	✓	OWN	OWN	OWN	✓
Delete	✓	OWN	OWN	OWN	✓
Download	✓	OWN	OWN	OWN	✓
Edit Metadata	✓	EDIT	EDIT	EDIT	✓
Export	✓	✓			✓
Import	✓	✓	✓		✓
Mobile Offline Viewing					
Re-stream	✓	✓	✓	✓	✓
Trim	✓	OWN	OWN	OWN	✓
View	✓	✓	✓	✓	✓

Videos Sessions Sources Layout Feed Analytics Administration

Tasks	Roles				
	Administrator	Content Creator	Content Contributor	Viewer	Set-Top Box
Access Control	✓	✓	✓	✓	✓
Change Sources	✓	OWN	OWN	OWN	✓
Create	✓	OWN	OWN	OWN	✓
Delete	✓	OWN	OWN	OWN	✓
Edit Metadata	✓	EDIT	EDIT	EDIT	✓
Live On/Off	✓	OWN	OWN	OWN	✓
Record	✓	OWN	OWN	OWN	✓
View Sessions	✓	✓	✓	✓	✓

Videos Sessions Sources Layout Feed Analytics Administration

Tasks	Roles				
	Administrator	Content Creator	Content Contributor	Viewer	Set-Top Box
Access Control	✓	OWN	OWN	OWN	
Create	✓	OWN	OWN	OWN	
Delete	✓	OWN	OWN	OWN	
Edit Metadata	✓	EDIT	EDIT	EDIT	
View	✓	✓	✓	✓	✓

[Videos](#)
[Sessions](#)
[Sources](#)
[Layout](#)
[Feed](#)
[Analytics](#)
[Administration](#)

Tasks	Roles				
	Administrator	Content Creator	Content Contributor	Viewer	Set-Top Box
Create	✓	✓			
Delete	✓	✓			
Edit	✓	✓			
View	✓	✓			

[Videos](#)
[Sessions](#)
[Sources](#)
[Layout](#)
[Feed](#)
[Analytics](#)
[Administration](#)

Tasks	Roles				
	Administrator	Content Creator	Content Contributor	Viewer	Set-Top Box
Change Content	✓	✓			✓
View	✓	✓	✓	✓	✓

[Videos](#)
[Sessions](#)
[Sources](#)
[Layout](#)
[Feed](#)
[Analytics](#)
[Administration](#)

Tasks	Roles				
	Administrator	Content Creator	Content Contributor	Viewer	Set-Top Box
View	✓				

[Videos](#)
[Sessions](#)
[Sources](#)
[Layout](#)
[Feed](#)
[Analytics](#)
[Administration](#)

Tasks	Roles				
	Administrator	Content Creator	Content Contributor	Viewer	Set-Top Box
Set-Top Box					✓

Customizing the Navigation Toolbar for Each Role

You can choose to hide items from the navigation toolbar for each role.

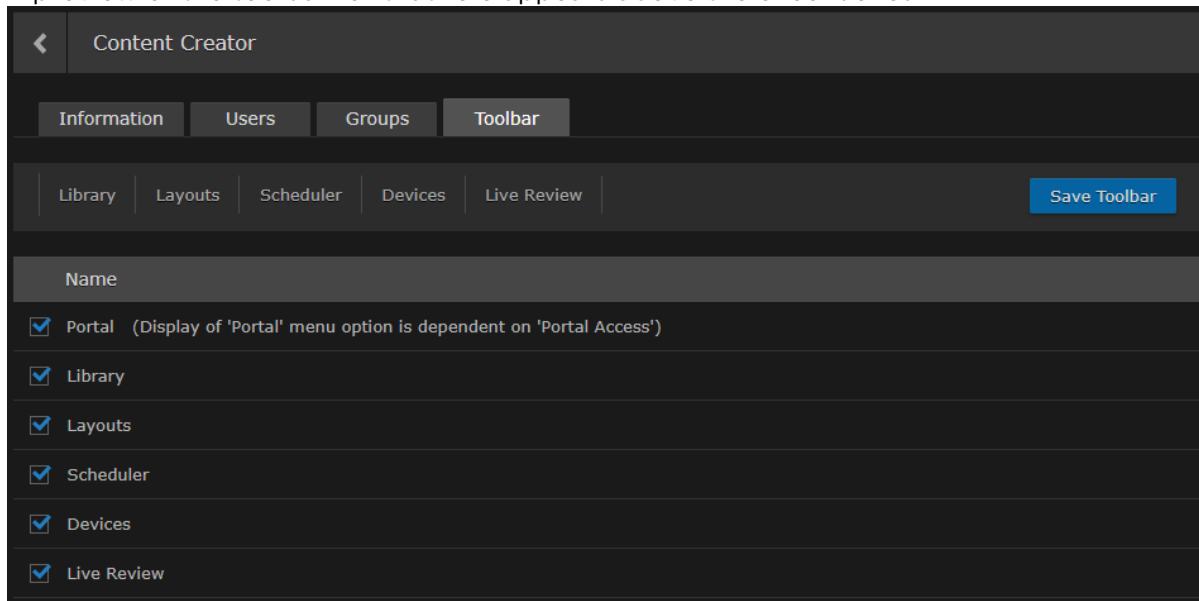
Tip

- The available items in the toolbar depend on your license.
- If a role does not have permission for a particular toolbar item, that takes precedence over the toolbar customization here. For example, if the role does not have the STB Administration permission and the toolbar customization setting for Devices is enabled, the Devices item does not appear in the navigation toolbar.

To customize the navigation toolbar for a role:

1. Select the role by clicking the role name.
2. On the Information pane, click the **Toolbar** tab.
3. On the Toolbar pane, click the checkboxes next to each item to enable/disable it from the toolbar.

A preview of the toolbar for that role appears above the checkboxes.



4. Click **Save Toolbar** to save the settings.

Managing Access Permissions

Note

Users can change the access permissions of items such as feeds, sources, videos, and sessions. Access permissions are defined on the Library's Access pane (by clicking the **Access** tab from the Information pane when adding or editing an item). You can specify access permissions on a per-user or per-group basis.

For information on the default permissions and the steps to change the access permissions of feeds, sources, videos, and sessions, see [Sharing Items](#) (in the [User's Guide](#)).

Administrators and other users may assign users access permissions for content rights (videos, sessions, sources, and feeds). Access permissions are combined with a user's role and may further qualify the user's privileges.


Permission needs to be granted on both the role AND access level in order for a user to have access. Basically, a user's role and access permission must match for the user to be able to do something.

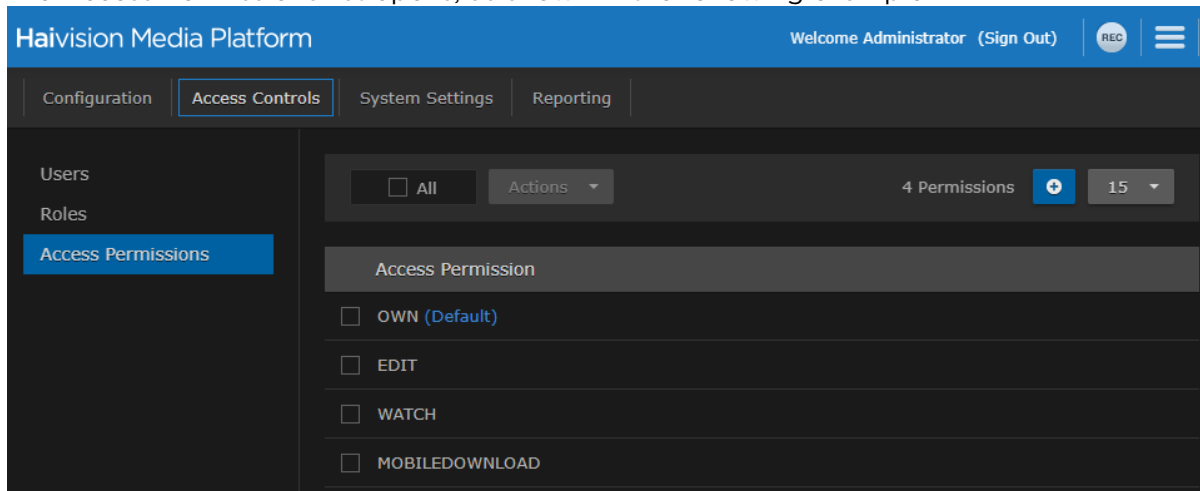
When setting up Haivision Media Platform, administrators can create custom access permissions. HMP provides the default access permissions shown below.

Important

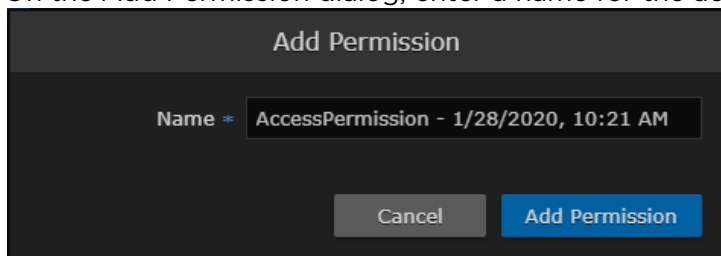
Depending on the Use Feed Permission setting, after an asset is selected for a feed, the feed access permissions take precedence over the permissions assigned to the asset. This means users may have access through feeds to assets that they would not have access to otherwise. For more information, see [Configuring Feeds and Activating the Portal](#).

To view and manage access permissions:

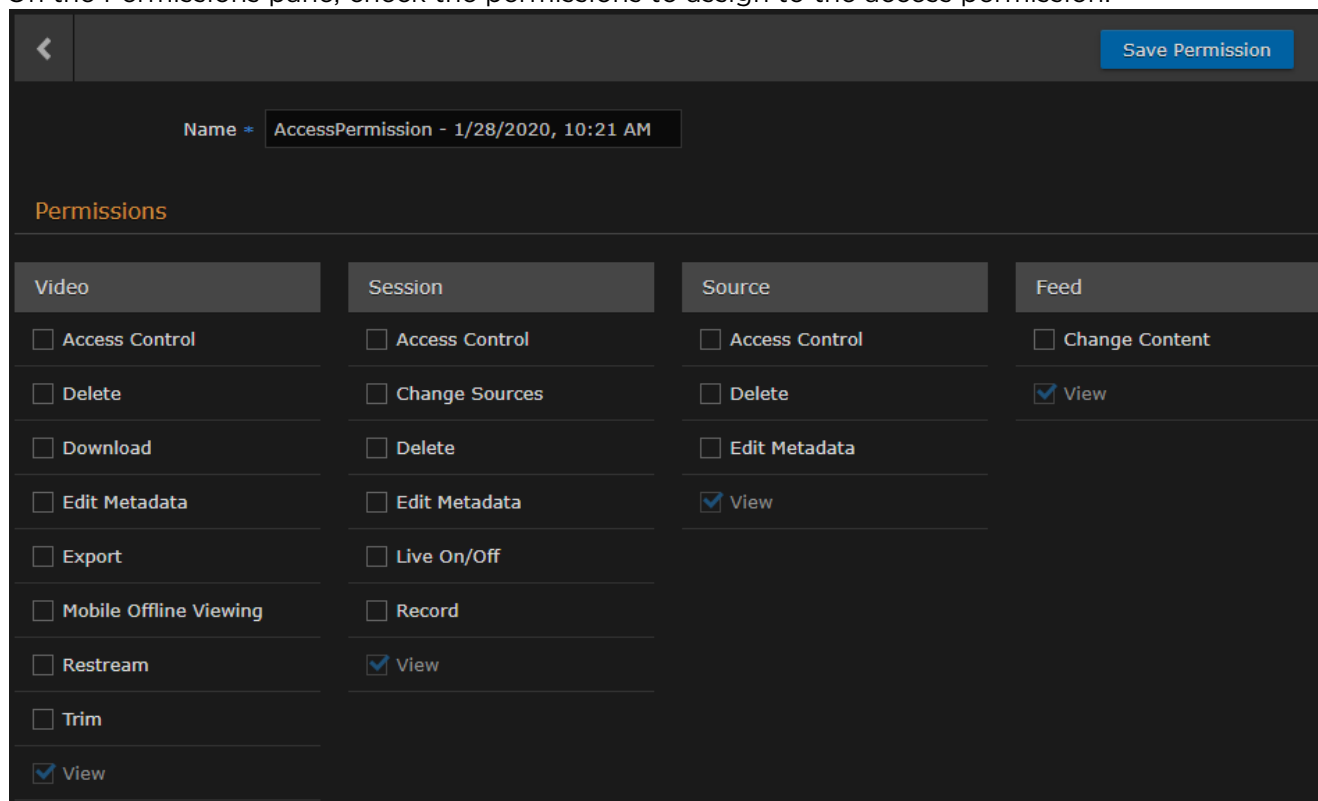
1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Access Controls** on the toolbar and then click **Access Permissions** on the sidebar. The Access Permissions list opens, as shown in the following example.




3. To create new a access permission, click the  icon.
4. On the Add Permission dialog, enter a name for the access permission and click **Add Permission**.



5. On the Permissions pane, check the permissions to assign to the access permission.



6. Click the **Save Permission** button.

7. Click the  icon to return to the Access Permissions list. This access permission is now available to users when changing permissions on videos, sessions, sources, or feeds.

Managing System Settings

This section describes how to manage your Haivision Media Platform (HMP) system settings, including authentication services, backup and restore, network settings, licensing, and security. It also provides the steps to install system updates.


Topics Discussed

- [Activating Command Line API Access](#)
- [Backing Up and Restoring HMP](#)
- [Managing Certificates](#)
- [Managing Directory \(Authentication\) Services](#)
- [Licensing Your HMP](#)
- [Configuring Network Settings](#)
- [Managing Network Storage](#)
- [Managing Security](#)
- [Installing System Updates](#)

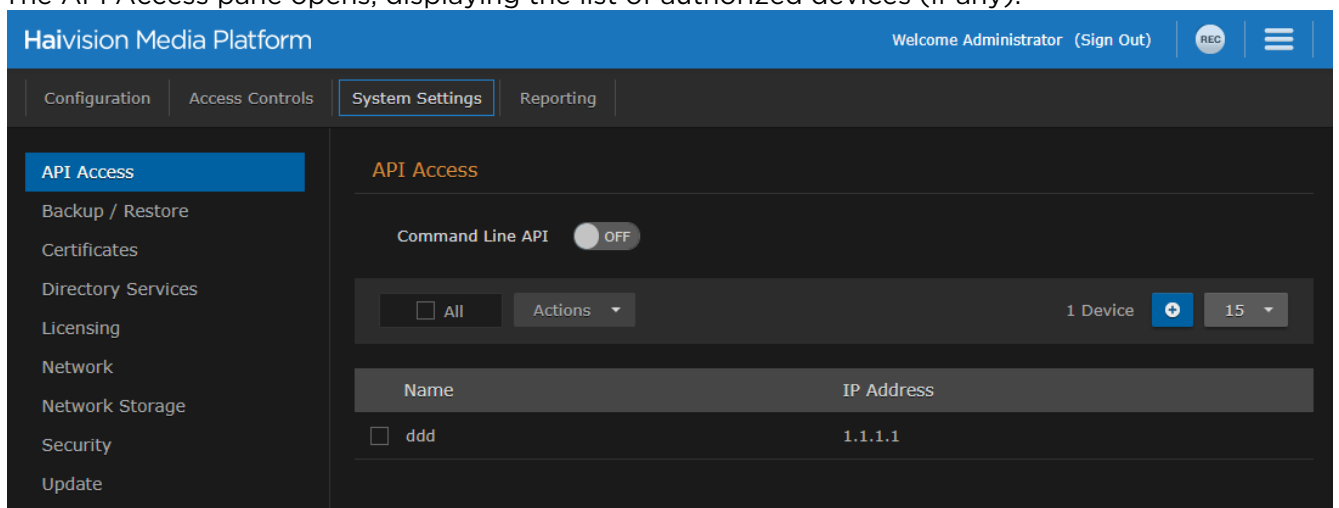
Activating Command Line API Access

Before using the Command Line API, you must activate Command Line API access on Haivision Media Platform and add the client devices to the list of authorized devices.

To enable Command Line API access on HMP:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **System Settings** on the toolbar and then click **API Access** on the sidebar.

The API Access pane opens, displaying the list of authorized devices (if any).



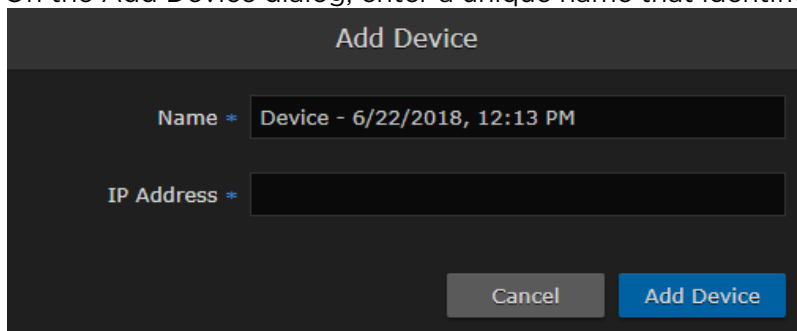
3. Toggle the Command Line API button to **On**.

Note

Toggling this button activates all devices in the list.

To add a device to the list:

1. Click the **+** icon.
2. On the Add Device dialog, enter a unique name that identifies this device.



3. Enter the IP address of the device that needs to access the Command Line API.
4. Click **Add Device**. The new device is added to the list of authorized devices.

Note

Further changes to the list of authorized devices are applied automatically. You do not need to restart HMP.

Backing Up and Restoring HMP

From the Backup/Restore pane, you can back up your Haivision Media Platform system configuration and permission information, either to a network storage location or your local server. The backup includes the local configuration, such as sources and sessions (but not LDAP user information).

From the Backup/Restore pane, you can schedule backups, configure the backup rotation, password-protect backups, view a list of backups, and restore backups. You can also download backup files and upload previously downloaded files.


Important

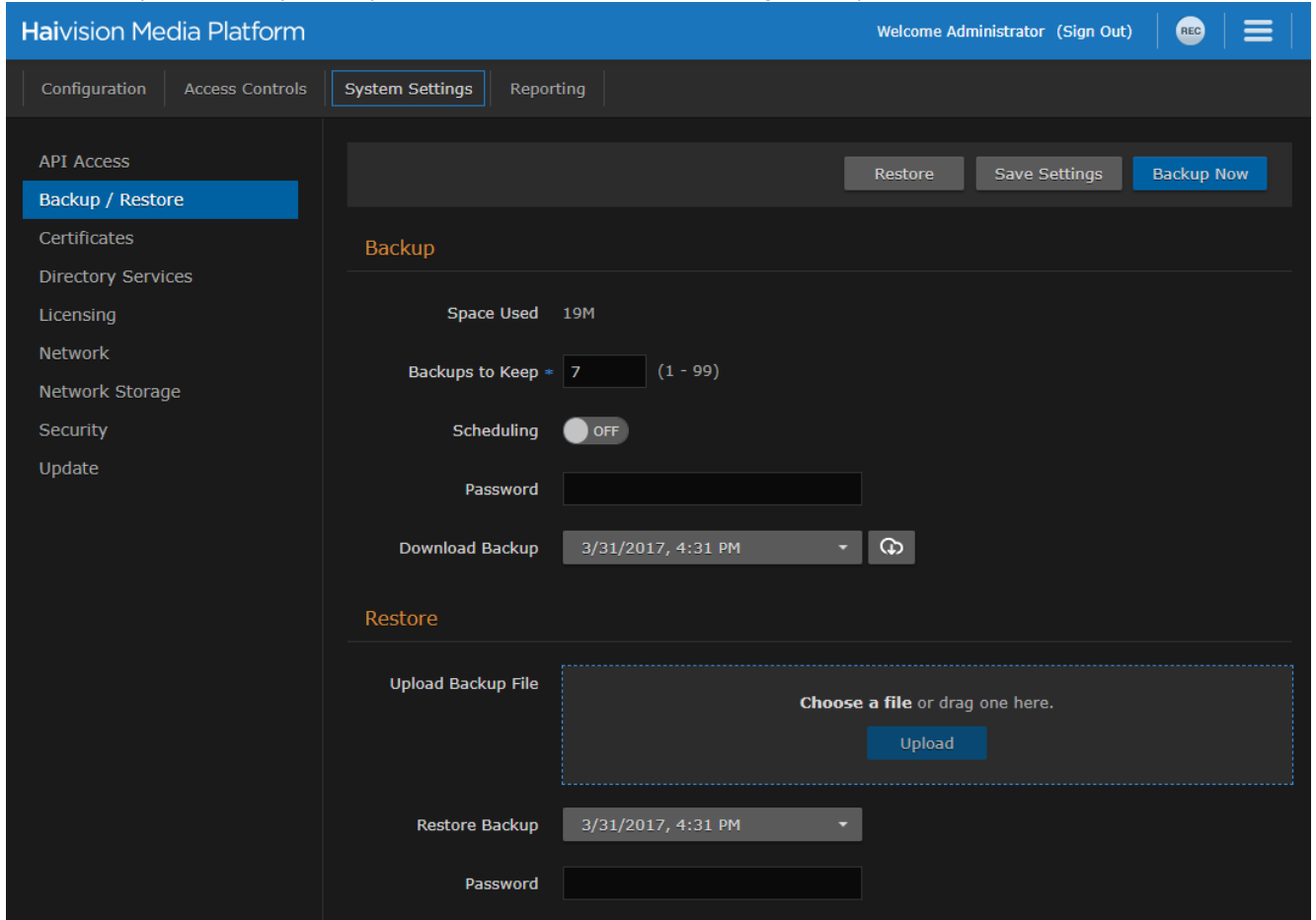
Changes to the number of backups to keep or the password, apply to immediate backups (Backup Now), but are *not* saved until you click **Save Settings**. When you refresh the page, restore a backup, or navigate away from the page, these changes are lost.

Tip

To back up files onto a Network File System (NFS) storage server, ensure NFS is set to On and configured. See [Managing Network Storage](#). Otherwise, backups are written to the local server.

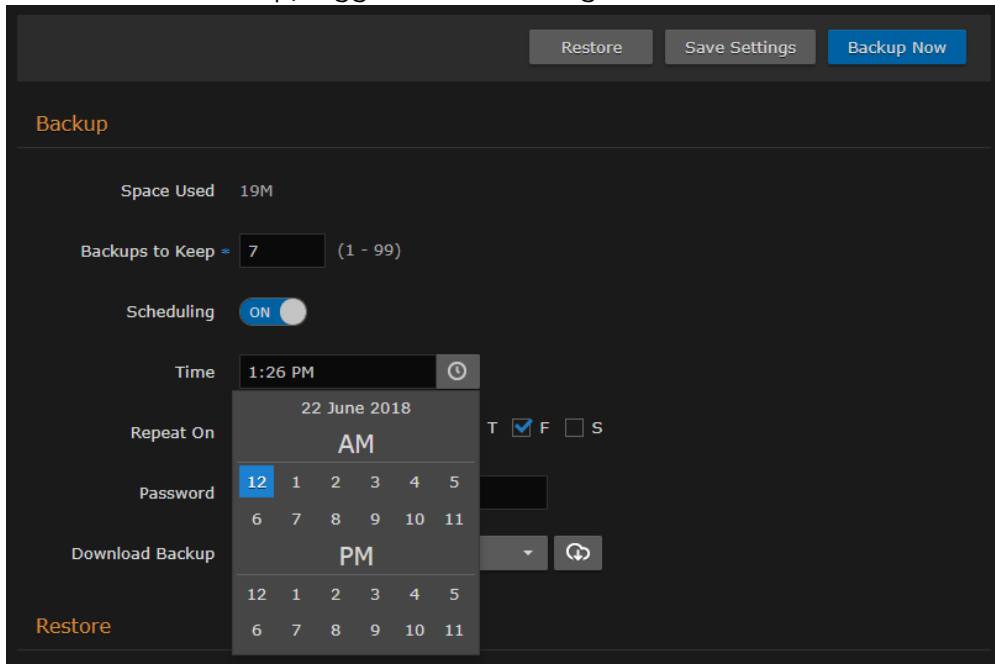
To configure and schedule backups:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **System Settings** on the toolbar and then click **Backup/Restore** on the sidebar. The Backup/Restore pane opens, as shown in the following example.

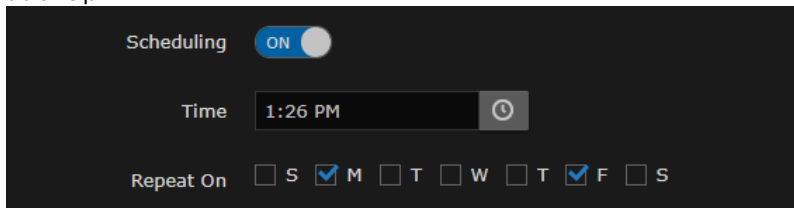


3. To configure the backup rotation (and manage your backup storage media), enter the number of backups to keep, from 1 to 99 (default is 7).

4. To schedule a backup, toggle the Scheduling button to **On** and select the start time.



5. To schedule recurring backups, check the checkbox next to the days on which to repeat the backup.



6. To password-protect the generated backup .zip file, enter a passphrase in the Password field. This password is required to restore the backup.

⚠ Important
If you lose your backup password, that backup file cannot be restored.

7. Click **Save Settings**.

Topics Discussed

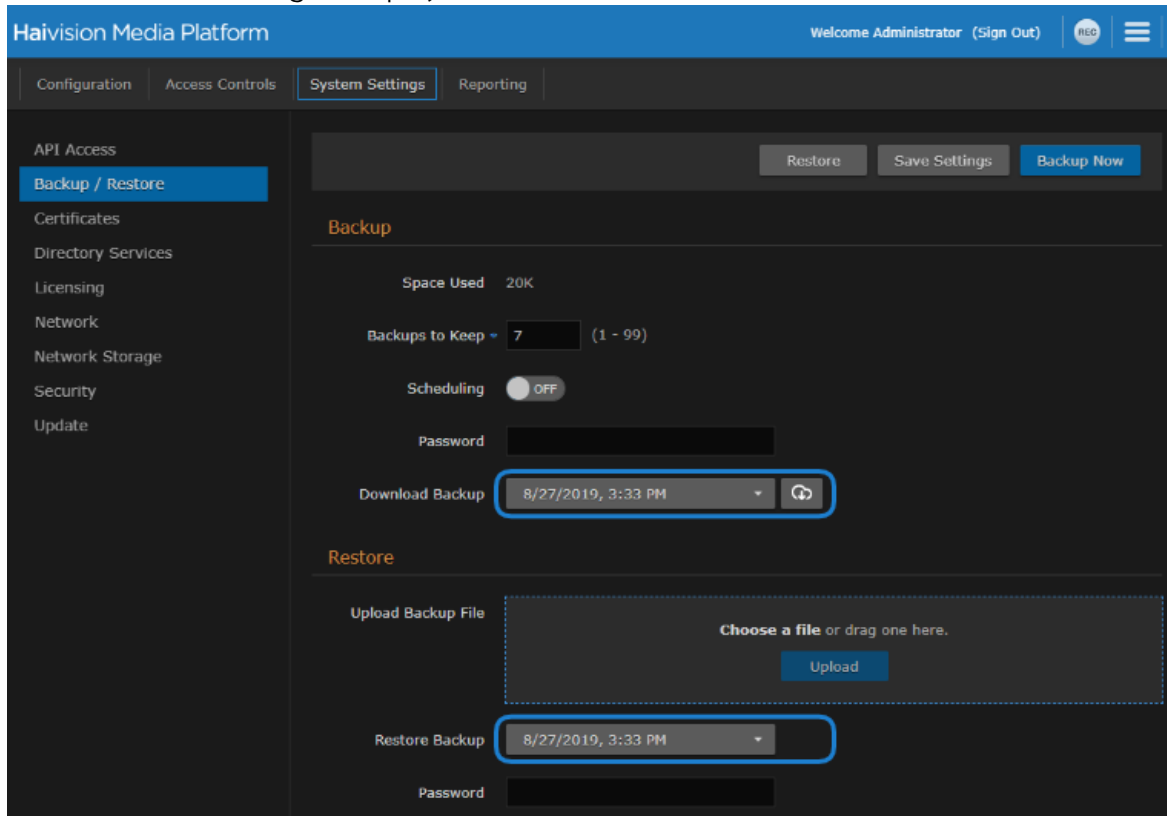
- [Backing Up HMP](#)
- [Uploading Backup Files](#)
- [Restore to a Previous Configuration](#)
- [Backup/Restore Settings](#)


Backing Up HMP

To back up HMP:

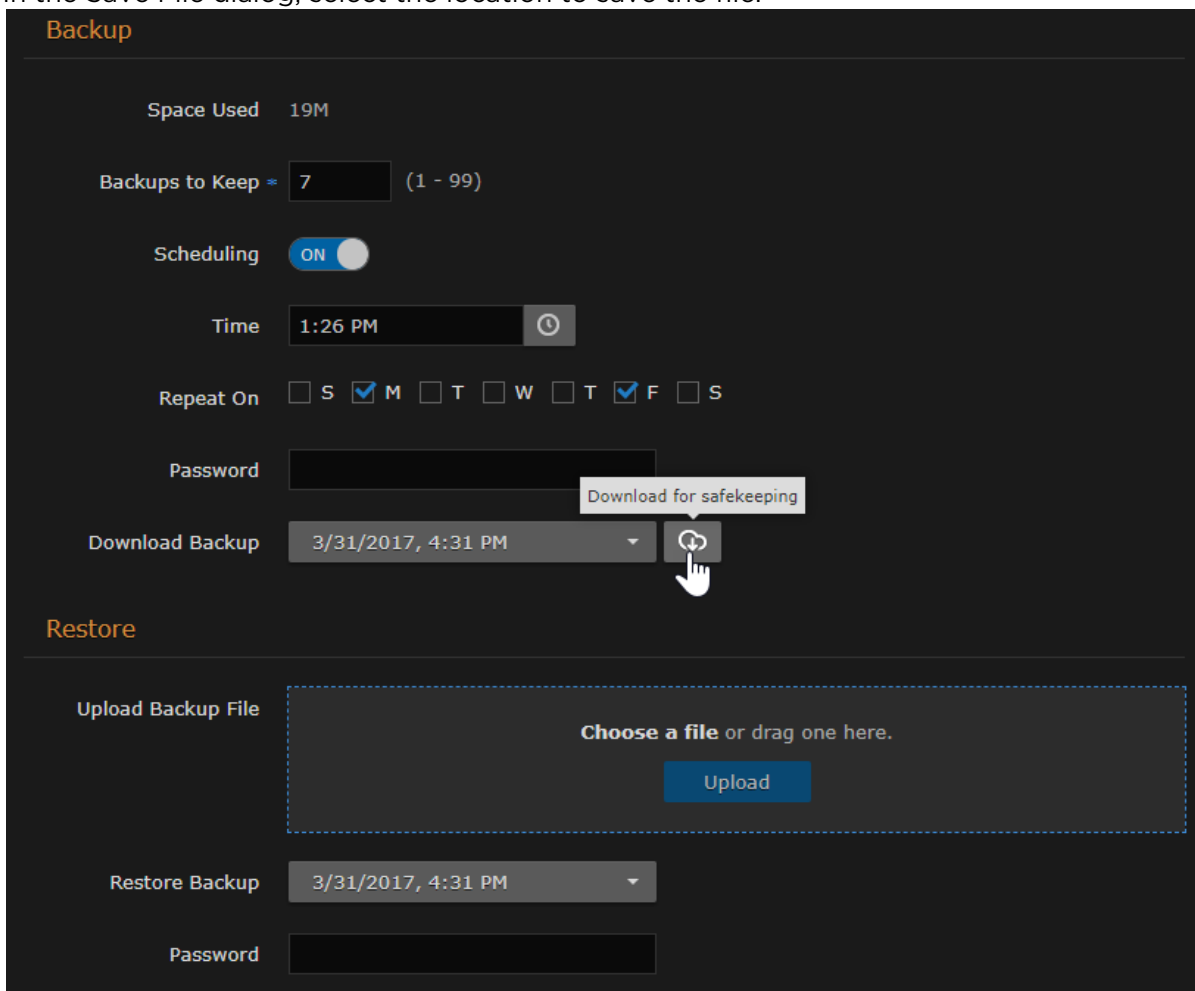
1. To back up your system immediately, click **Backup Now**.
HMP backs up your local configuration and permissioning information and adds the new file to the Download Backup and Restore Backup drop-down lists (available after backup completes, as

shown in the following example).



2. To download a backup file to your local computer for safekeeping:
 - a. Select the file from the Download Backup list.
 - b. Click the  icon.

c. In the Save File dialog, select the location to save the file.



The generated backup file is a .zip file with the following syntax: backup-*nnnnnnnnnn*.zip.

Uploading Backup Files

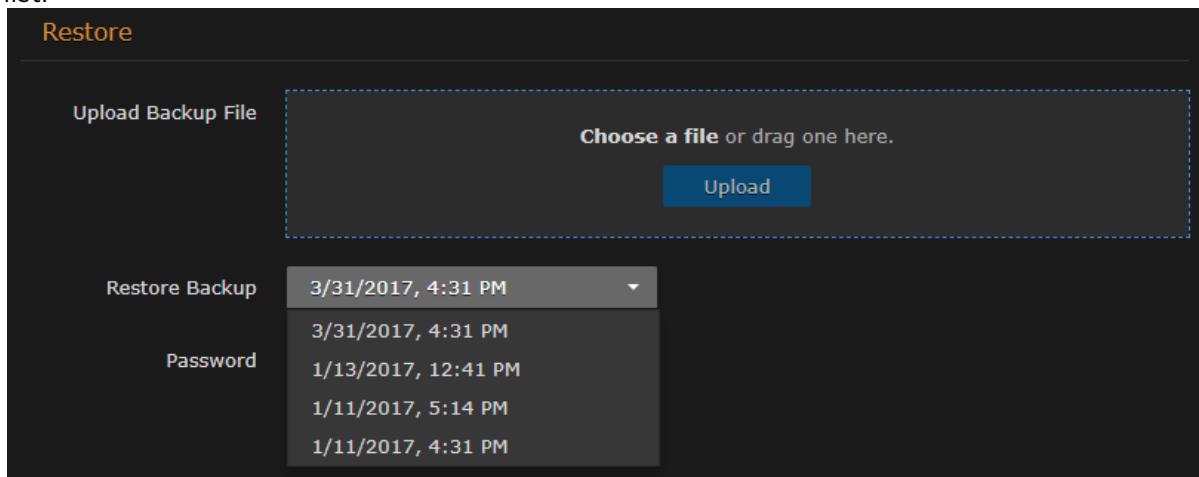
To upload a previously downloaded backup file:

1. On the Backup/Restore pane, drag a file to the drop area or click **Choose a file**, and select a file to upload in the Open File dialog.
The backup file must be a .zip file with the following syntax: backup-*nnnnnnnnnn*.zip.
2. Click **Upload**. The file is now added to the Download Backup and Restore Backup lists.

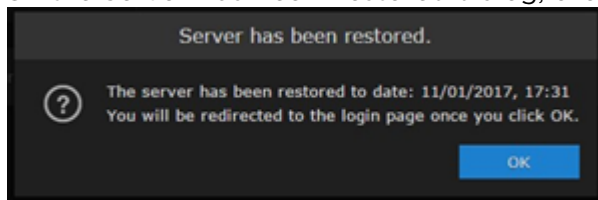
Restore to a Previous Configuration

To restore HMP to a previous configuration:

1. On the Backup/Restore pane, select the backup file to restore from the Restore Backup drop-down list.

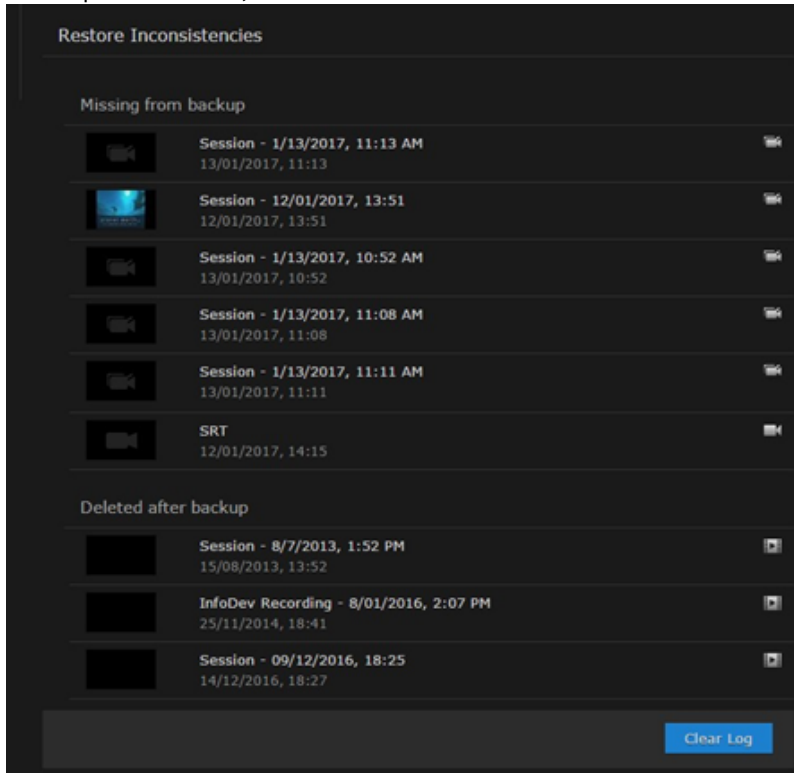


2. If the file is password-protected, enter the password in the Password field.
3. Click **Restore**, and then click **Confirm**.
4. On the Server Has Been Restored dialog, click **OK** to proceed.



5. Wait until the update completes and HMP restarts. After the appliance restarts, the browser displays the HMP Sign-in screen. If not, refresh your browser.

- If changes have been made to the HMP's sources, sessions, videos, or layout images since the backup was made, the inconsistent items are listed under Restore Inconsistencies.



- You can click the link (such as the video shown in the above example), to open the Content Browser, view and optionally restore the change.
- When you are satisfied with the restore, return to the Backup/Restore pane and click **Clear Log**.

Backup/Restore Settings

The following table lists the configurable Haivision Media Platform Backup/Restore settings.

[Backup](#) [Restore](#)

Setting	Default	Description
Space Used	—	The amount of disk/file spaced used for backups.
Backups to Keep	7	The number of backups to keep. When the maximum number is reached, HMP deletes the oldest file to make room for the newest. Range: 1-99
Scheduling	Off	To schedule backups, toggle the Scheduling button to On . The Time and Repeat On fields then become available.
Time	Current time	(Scheduling must be On) Type or use the calendar to adjust the start date and time.
Repeat On	Current day	(Scheduling must be On) To configure recurring backups, check the checkboxes for the days of the week to repeat the backup.
Password	—	To password-protect the backup, enter a password that will be required to restore the backup.
Download Backup	—	(Available after creating a backup) Select a backup file to download from the drop-down list of download dates.

[Backup](#) [Restore](#)

Setting	Default	Description
Upload Backup File	—	To upload a previously downloaded backup file, click Browse and select the .zip file.
Restore Backup	—	Select the backup to restore from the drop-down list of backup files.
Password	—	If the backup is password-protected, enter the password for the file.

Managing Certificates

From the Certificates pane, you can generate an SSL private key and certificate signing request (CSR). You can then import the signed certificate and trust chain returned by the Certification Authority (CA).

The Certificates pane lists the Identity Certificates available on Haivision Media Platform. An Identity Certificate identifies the device during the authentication process when trying to establish a TLS connection in HTTPS session startup. Its Common Name or Alternate Subject Names must match its IP address and/or its FQDN (Fully Qualified Domain Name) if DNS is used.


The default certificate is localhost.crt (self-signed).

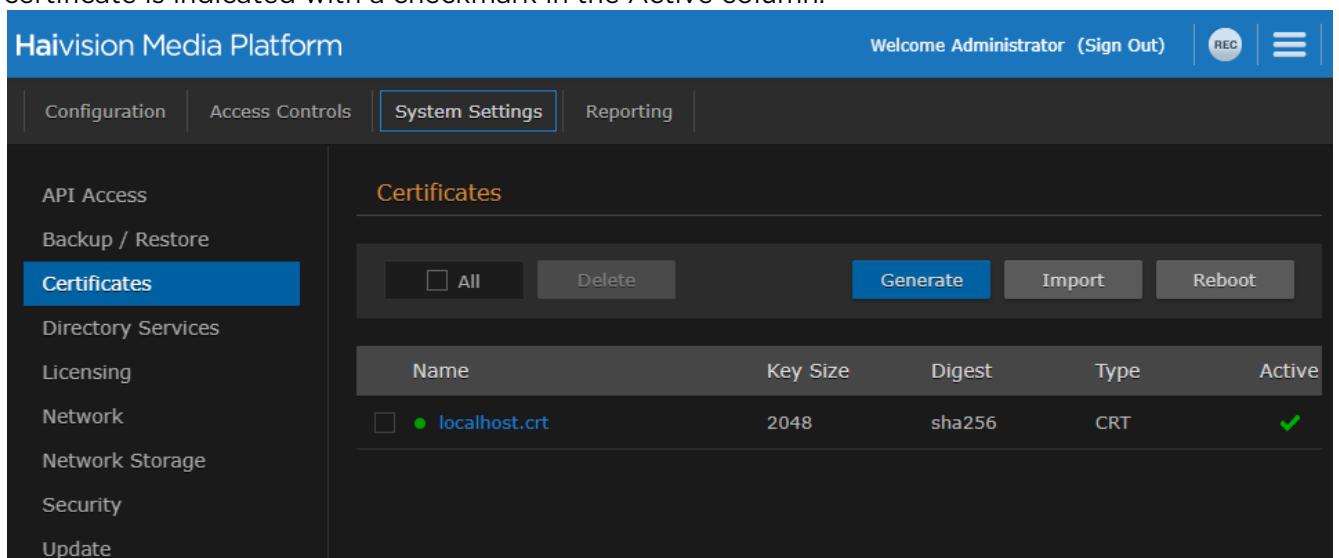
Topics Discussed

- [Generating a Certificate Signing Request \(CSR\)](#)
- [Importing and Activating a Certificate \(CRT\)](#)
- [Generating a Private Key](#)
- [Importing a Private Key](#)
- [Generating a New Self-Signed Certificate](#)
- [Certificate Settings](#)

Generating a Certificate Signing Request (CSR)

To generate a Certificate Signing Request (CSR):

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **System Settings** on the toolbar and then click **Certificates** on the sidebar. The Certificates pane opens, listing any certificate signing requests generated on HMP. The active certificate is indicated with a checkmark in the Active column.



3. Click **Generate**.

4. On the Generate Certificate or Private Key dialog, enter a name for the certificate.

5. Ensure the Type is Certificate Signing Request and complete the remaining fields. See [Certificate Settings](#).

- For the Subject, enter information about the device that the Identity Certificate represents. For more information, see the "Subject" entry in [Certificate Settings](#).

6. Click **Generate**.

7. Returning to the Certificates list, click the link for the generated CSR to open the file in a new window. Copy the contents (including both beginning and ending delimiters) and paste it into your Certificate Authority (CA) application. The CA will return an intermediate certificate (trust chain) and signed certificate (CRT).

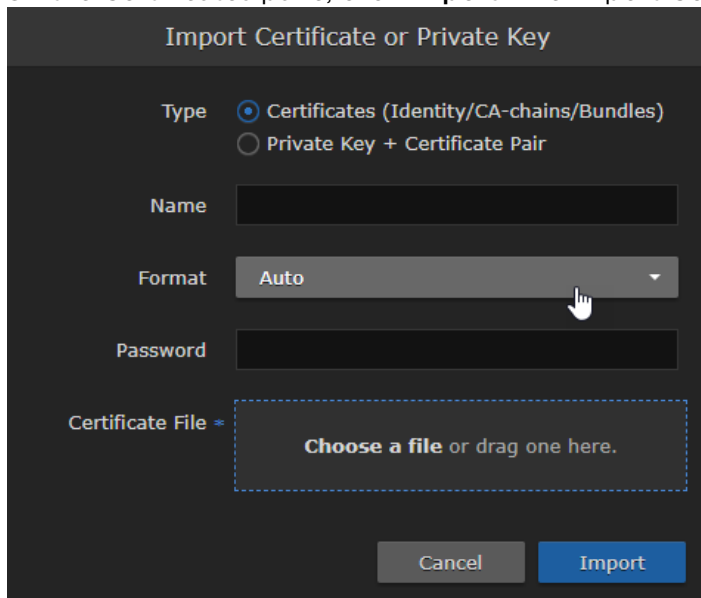
Tip

Keep in mind that there is a difference between importing a new certificate (that was generated externally) and importing a newly signed certificate whose request was previously generated on HMP and exported for signing.

Importing and Activating a Certificate (CRT)

To import and activate a Certificate (CRT):

1. On the Certificates pane, click **Import**. The Import Certificate or Private Key dialog appears.



2. Ensure Certificates (Identity/CA-chains/Bundles) is selected as Type.
 3. Enter the certificate name and remaining fields. See [Certificate Settings](#) for details.
 4. If your certificate is encrypted, enter the password.
 5. Drag a CA-signed certificate (CRT) to the drop area or click **Choose a file** and select the certificate.
 6. Click **Import**.
On the Certificates pane, the newly imported certificate is added to the list and should have a green status LED.
 7. In the row for the imported certificate, click in the Active column to activate the certificate.
 8. Click **Reboot** and click **Confirm** if you have changed the active certificate.
- A dialog appears informing you when the reboot is complete.

Generating a Private Key

To generate a Private Key:

1. On the Certificates pane, click **Generate**.
2. On the Generate Certificate or Private Key dialog, enter a name for the certificate.
3. For the Type, select **Self-Signed**.
4. Check the Create New Private Key checkbox.

Generate Certificate or Private Key

Name * Haivision

Type Self-Signed

Create New Private Key
Generating a new private key will overwrite the current private key.

Key Length 2048

Digest Algorithm SHA-256

Subject * /C=US/ST=Illinois/L=Lake Forest/O=Haivis

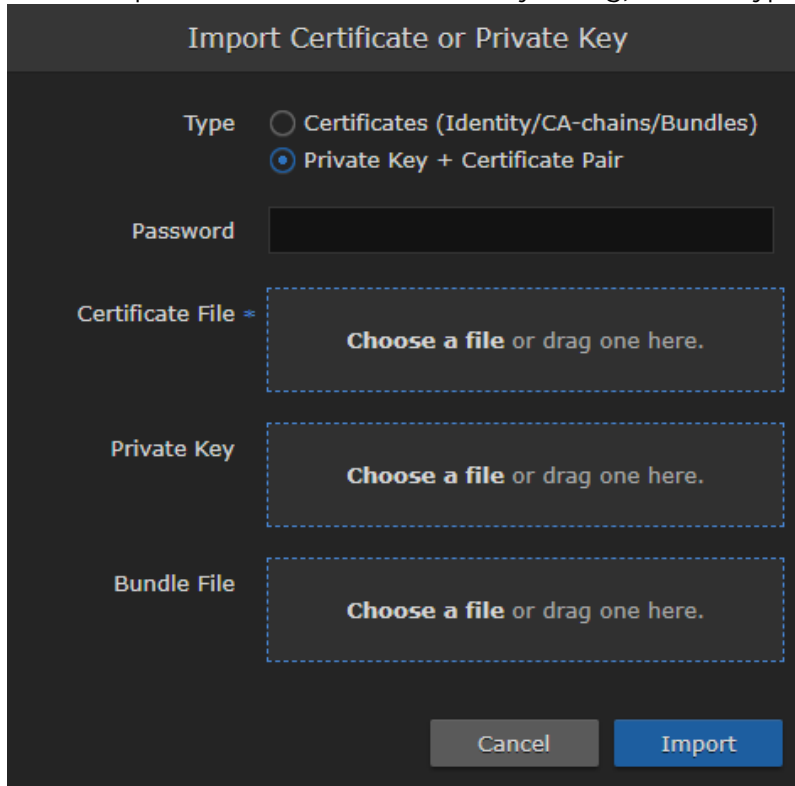
Cancel Generate

5. Fill in the remaining fields. See [Certificate Settings](#) for details.
 6. Click **Generate**.
 7. In the Certificates page, the newly imported certificate is added to the list and should have a green status LED. Click in the Active column to activate the certificate.
 8. Click **Reboot** and click **Confirm** for the new certificate to take effect.
- A dialog appears informing you when the reboot is complete.

Importing a Private Key

To import a private key:

1. On the Certificates pane, click **Import**.
2. On the Import Certificate or Private Key dialog, for the Type select **Private Key + Certificate Pair**.



Import Certificate or Private Key

Type Certificates (Identity/CA-chains/Bundles)
 Private Key + Certificate Pair

Password

Certificate File

Private Key

Bundle File


3. Enter the password for the private key.
4. To update your security certificate, drag the new SSL Certificate and SSL Certificate (Private) Key, and optionally an SSL Intermediate Certificate Bundle file to the drop area or click **Choose a file**.
5. Click **Import**. On the Certificates pane, the newly imported files is added to the list.
6. Click **Reboot** and click **Confirm** for the new certificate to take effect.

A dialog appears informing you when the reboot is complete.

Generating a New Self-Signed Certificate

If you have upgraded from a previous HMP version to version 3.1 or greater, due to a new restriction of TLS certificates in certain operating systems, a new self-signed certificate with a 2-year expiration should be generated after the upgrade.

To generate a new self-signed certificate:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **System Settings** in the admin toolbar, and click **Certificates** in the sidebar.
3. Click the **Generate** button.
4. On the Generate Certificate or Private Key dialog:
 - a. Enter a name for the certificate.
 - b. For the Type, select **Self-Signed**.
 - c. Fill in the remaining fields. See [Certificate Settings](#).
 - d. Click the **Generate** button.
5. The new certificate is added to the Certificates list.
6. Select the new certificate in the Active column to activate it.
7. Optionally, delete the old certificate.
8. Click **Reboot** and click **Confirm** for the change to take effect.

A dialog appears informing you when the reboot is complete.

Certificate Settings


The following table lists the configurable Haivision Media Platform Certificate settings.

 **Note**

Please contact your Network Administrator if you are unsure what to enter in any of these fields or if you are unsure whether the setting is required on your network.

[Generate Certificate or Private Key](#) [Import Certificate](#)

Setting	Description
Name	Enter a unique name under which the certificate is stored on HMP, as well as listed on the Certificate pane
Type	Select the Signature Type: <ul style="list-style-type: none"> • Self-signed: The certificate is generated and signed by the system, and the name is added to the list of Identity Certificates. • Certificate Signing Request: A request is generated, and its name is added to the list of Identity Certificates. The request is located in your home directory (accessible through the CLI), or you may export it by clicking on the View button and copying the content into a new file in a text editor. In its generated form, this certificate is still a request and cannot be used as an Identity Certificate before it is signed by a CA, and imported back.
Digest Algorithm	Select the digest algorithm (Secure Hash Algorithm): <ul style="list-style-type: none"> • SHA-256 • SHA-384 • SHA-512

Setting	Description
Subject	<p>The Subject identifies the device being secured, in this case, HMP. Enter the subject in the form: "/C=.../ST=.../L=.../O=.../OU=.../CN=..." where the most common attributes are:</p> <ul style="list-style-type: none"> • /C Two Letter Country Name • /ST State or Province Name • /L Locality Name • /O Organization Name • /OU Organizational Unit Name • /CN Common Name <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p> Tip For successful authentication, the Common Name in the certificate should be the IP address (by default) or domain name of the device.</p> </div>
V3 Extension	<p>V3 extensions allow more configuration options to be inserted in the Code Signing Request, such as alternative subject names and usage restrictions to certificates. See SSL Certificates and Subject Alternative Names for more details.</p> <p>To add one or more Subject Alternative Names, enter the same information that would go in the extensions section of an OpenSSL configuration file. For example:</p> <pre style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> [req] req_extensions = v3_req [v3_req] # Extensions to add to a certificate request subjectAltName = @alt_names [alt_names] DNS.1 = server1.example.com DNS.2 = mail.example.com DNS.3 = www.example.com DNS.4 = www.sub.example.com DNS.5 = mx.example.com DNS.6 = support.example.com </pre>

Generate Certificate or Private Key [Import Certificate](#)

Setting	Description
Type	<p>Select the certificate type:</p> <ul style="list-style-type: none"> • Certificates: (Identify/CA-chains/Bundles) • Private Key + Certificate Pair
Name	Name of the certificate.
Format	<p>Select the file format for the certificate (The formats differ in the way the file is encrypted):</p> <ul style="list-style-type: none"> • Auto: Detected from the file extension • der (Distinguish Encoding Rules) • pkcs #7 • pkcs #12
Password	If the imported certificate contains a password-protected private key, type its password in this field. Leave this field empty if the file is not password-protected.
Certificate File	Drag a certificate file to the drop area or click Choose a file to choose a file to upload.

Managing Directory (Authentication) Services

Haivision Media Platform allows you to connect to your LDAP or Active Directory server for user accounts.

⚠ Important

- If Haivision Media Platform is connected to an LDAP or Active Directory server, the users and groups lists is populated with information from the directory server. In an LDAP/AD environment, you cannot add or modify users or groups directly from HMP.
- LDAP and Active Directory are used for authentication purposes only. No HMP data is stored or changed on these systems.


You can also integrate HMP with an Active Directory-based single sign-on (SSO) environment. For details, see [Integrating HMP with Single Sign-On \(SSO\) Environments](#).

Topics Discussed

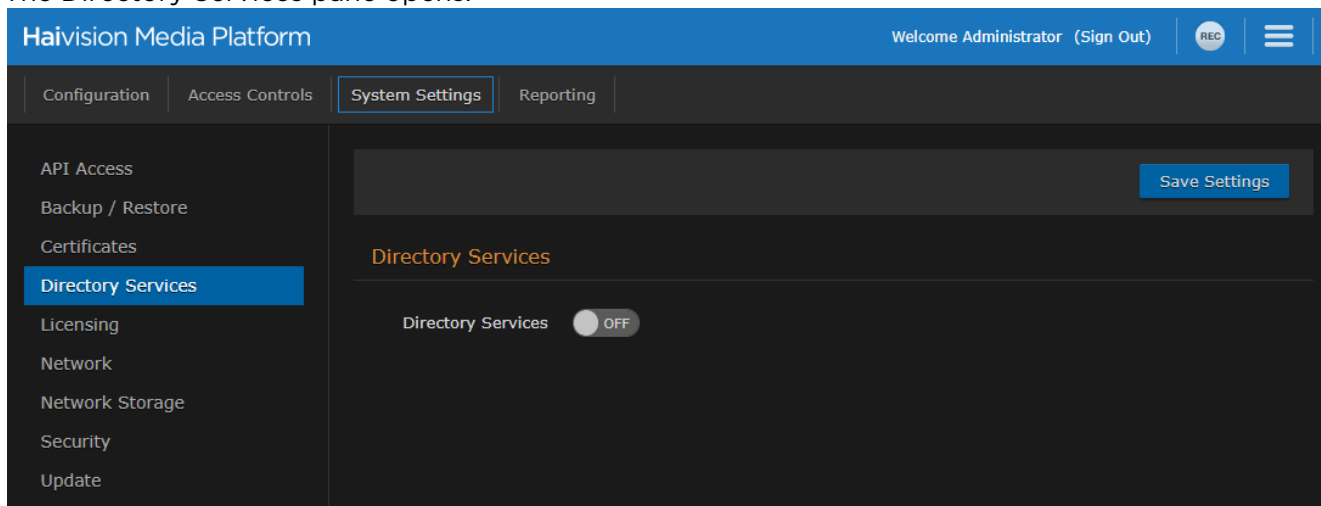
- [Connecting to a Directory Server](#)
- [Disconnecting from a Directory Server](#)
- [Directory Service Settings](#)
- [Integrating HMP with Single Sign-On \(SSO\) Environments](#)
- [Single Sign-On \(SSO\) Settings](#)

Connecting to a Directory Server

To connect HMP to a Directory Server:

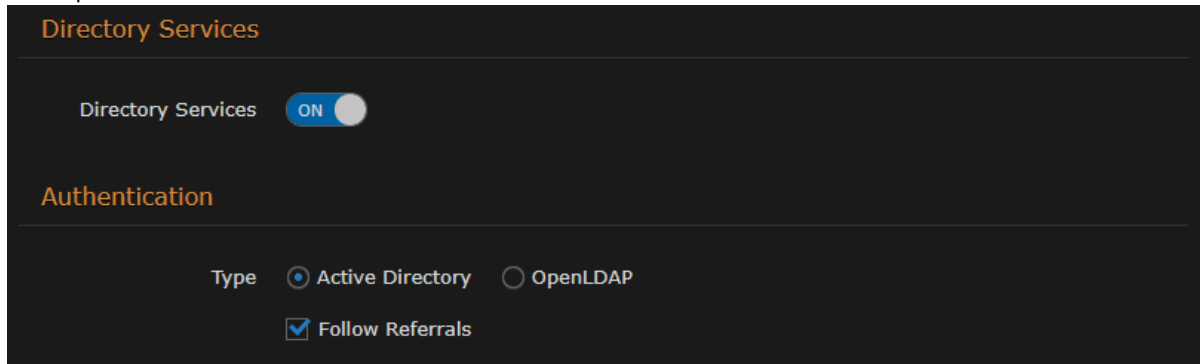
1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **System Settings** on the toolbar and then click **Directory Services** on the sidebar.

The Directory Services pane opens.

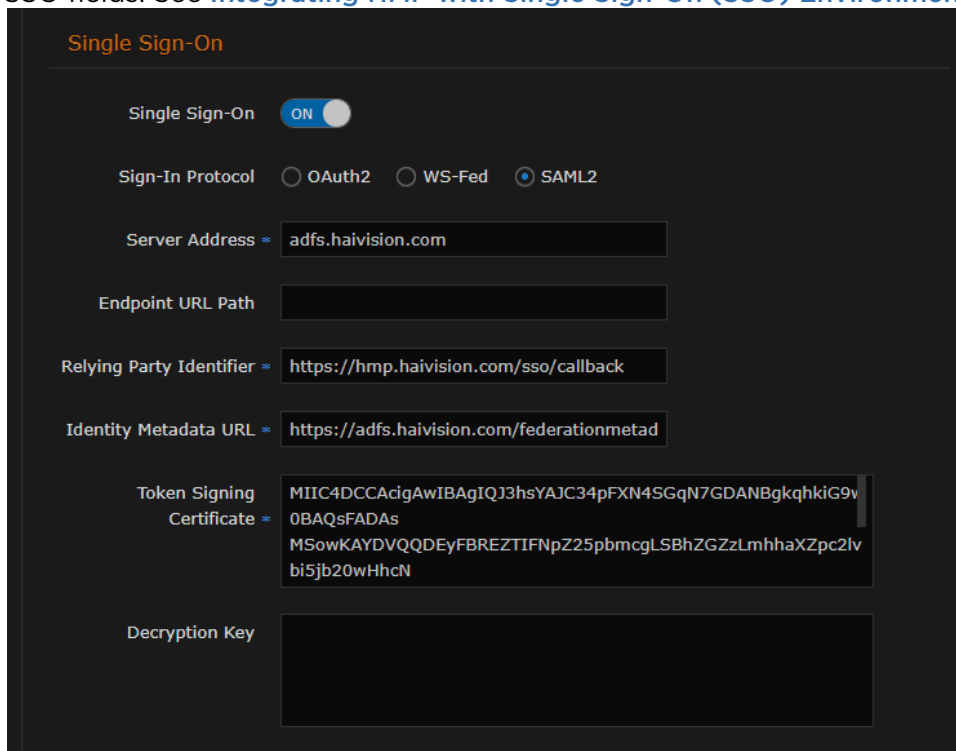


3. To connect to an LDAP or Active Directory server, toggle the **Directory Services** button to **On**. The Directory Services configuration settings then become available, as shown in the following

example.



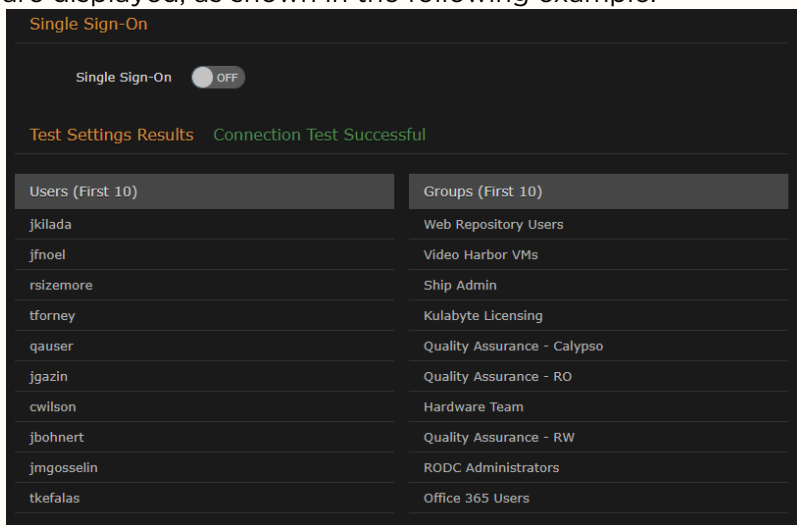
4. Under Authentication, select the type of LDAP implementation for your system, either:
 - Active Directory: An implementation of LDAP directory services by Microsoft.
 - OpenLDAP: An open source implementation of LDAP directory services.
5. For the server Connection, Query, and Data Mapping settings, enter or select the new values in the appropriate fields. See [Directory Service Settings](#) for details.
6. To configure Single Sign-On (SSO), toggle the Single Sign-On button to **On**. The SSO configuration settings appear, as shown in the following example. Enter or select the appropriate values in the SSO fields. See [Integrating HMP with Single Sign-On \(SSO\) Environments](#).



7. To test the connection to the defined directory server, click the **Test Settings** button.

Note

- If you get the message "Anonymous Connection Succeeded," this means that HMP has found the server, but the username and/or password is most likely wrong.
- If you get the message "Connection Test Succeeded," this means that the server IP address, port, username, and password are correct. A list of the first 10 users and groups are displayed, as shown in the following example.



8. Click **Save Settings** to save the connection.

The users and groups lists are populated with the LDAP or Active Directory users and groups.

For more information, see [Managing Users](#) and [Managing Groups \(LDAP/AD Only\)](#).

Disconnecting from a Directory Server


To disconnect HMP from a Directory Server:

1. On the Directory Services pane, toggle the Directory Services button to **Off**.
2. Click **Save Settings**.
HMP removes the LDAP or Active Directory information, and the Users and Groups panes return to the local account lists.

Directory Service Settings


The following table lists the Directory Service settings.

[Authentication](#) [Connection](#) [Query](#) [Data Mapping](#) [Single Sign-On](#)






Setting	Default	Description/Values
Type	Active Directory	Select your authentication server type: <ul style="list-style-type: none"> • Active Directory • OpenLDAP
Follow Referrals	Enabled	Referral following is enabled when this checkbox is checked (default). <ul style="list-style-type: none"> • When enabled and HMP's LDAP client searches for users or groups, it recursively creates new connections to search other servers referenced by the Directory Services server that is currently being searched. • When disabled, the LDAP client does not connect to any other servers besides the one specified by the Connection settings. <div style="border: 1px solid #c8e6c9; padding: 5px; margin-top: 10px;"> <p> Tip In certain environments, you may want to disable referrals: For example, in troublesome environments or in places where referral servers do not add any useful information about the configured users.</p> </div>

[Authentication](#) [Connection](#) [Query](#) [Data Mapping](#) [Single Sign-On](#)

Setting	Default	Description/Values
IP Address	—	The IP address or domain name of the server that hosts the authentication server.
Port	389	The communications port that the authentication service uses. The default value is 389 (the standard port used for LDAP connections). The default is 636 for SSL connections.
Connection	Basic	Select the encryption protocol: <ul style="list-style-type: none"> • Basic: Unencrypted connection • SSL: Secure Socket Layer (recommended)
Username	—	The username for HMP to connect to your authentication system and query it for the required information. The user account needs to have permission to connect to the server and read the information in the authentication directory.
Password	—	The password that corresponds with the user name provided for the Username field.

Setting	Default	Description/Values
Sync Interval	60 minutes	<p>The directory server sync interval.</p> <div style="border: 1px solid green; padding: 5px;"> <p> Tip</p> <ul style="list-style-type: none"> • Changing this value triggers a sync of the directory server. • We recommend setting this value to once per day (1440 minutes). </div>

[Authentication](#)
[Connection](#)
[Query](#)
[Data Mapping](#)
[Single Sign-On](#)

Setting	Default	Description/Values
Base DN	—	<p>The Base DN (Distinguished Name) used by your authentication system. This setting should be provided by your AD/LDAP administrator. For example: <code>ou=staff,dc=haivision,dc=com</code></p> <div style="border: 1px solid yellow; padding: 5px;"> <p> Note</p> <p>Spaces are not allowed unless they are part of the path.</p> </div> <div style="border: 1px solid yellow; padding: 5px;"> <p> Important</p> <p>If the Base DN is wrong, HMP is not able to access the groups. When the connection test succeeds, a list of the first 10 users and groups appears. (See example in Connecting to a Directory Server.)</p> </div>
User Context	—	<p>The DN of the context (container) where your authentication system users can be found. This setting should be provided by your AD/LDAP administrator. For example: <code>ou=people,dc=haivision,dc=com</code></p> <div style="border: 1px solid yellow; padding: 5px;"> <p> Important</p> <p>If the User Context is wrong, users are not able to sign in correctly. For example, they may only have the anonymous privileges or even a blank screen.</p> </div> <div style="border: 1px solid yellow; padding: 5px;"> <p> Note</p> <p>To simplify management of user bases, you can specify separate search bases for User and Group objects. You can also input multiple User Contexts (separated by line feeds, i.e., each line is a new context).</p> </div>
Group Context	—	<p>The DN of the context where your authentication system groups can be found. This setting should be provided by your AD/LDAP administrator.</p> <div style="border: 1px solid yellow; padding: 5px;"> <p> Note</p> <p>See previous note to input multiple Group Contexts.</p> </div>
User Attribute	sAMAccountName	<p>The user attribute your directory system uses. OpenLDAP systems normally use <code>cn</code> or <code>uid</code>. Active Directory systems normally use <code>sAMAccountName</code>; However, <code>userPrincipalName</code> is also supported for signing in using email addresses.</p>

Setting	Default	Description/Values
Member Attribute	memberOf	The member attribute your directory system uses. OpenLDAP systems normally use <code>member</code> or <code>memberUid</code> , while Active Directory systems normally use <code>memberOf</code> .
Group Object Class	((objectClass=group) (objectClass=groupOfNames))	Object class query for groups. The default works with almost all directory servers
User Object Class	(objectClass=person)	Object class query for users. The default works with almost all directory servers.
Query Page Size	1000	Sets the size of a page for paged results. Paged results are typically supported, but the supported page size may need to be configured for your site. If the requested size is not supported by the LDAP server, a non-paged query is attempted. The default on most directory servers is 1000.

[Authentication](#)
[Connection](#)
[Query](#)
[Data Mapping](#)
[Single Sign-On](#)

Setting	Default	Description/Values
Group Name	cn	HMP needs these fields to read from the directory server. The defaults should work on most systems. If your system uses different attribute names, configure them here.
Display Name	displayName	
Email	mail	
User Principal Name	userPrincipalName	

[Authentication](#)
[Connection](#)
[Query](#)
[Data Mapping](#)
[Single Sign-On](#)

Setting	Default	Description/Values
Single Sign-On	Off	To configure Single Sign-on, see Integrating HMP with Single Sign-On (SSO) Environments .

Integrating HMP with Single Sign-On (SSO) Environments

You can integrate Haivision Media Platform with an Active Directory-based Single Sign-On (SSO) environment, specifically Active Directory Federation Services (AD FS) and Azure AD. This feature is designed to provide authentication and identity management simplification and centralization.

Single Sign-On enables users to move between services securely and uninterrupted without specifying their credentials each time. After your users sign into their directory server, they are automatically granted access to HMP.

HMP's browser-based SSO implementation supports the following standard identity protocols: Security Assertion Markup Language (SAML2), WS-Federation, and OAuth2.

- WS-Fed and SAML2 work for Windows Server 2008+ / AD FS 2.0+ and Azure,
- OAuth2 works for Windows Server 2012 R2 / AD FS 3.0+ and Azure.

With Azure AD, you must use a Windows Server with Azure AD Connect for Directory Services configuration. The current HMP release does not support SSO for users created directly on Azure AD, and must be able to query a traditional Active Directory system for user and group details after being authorized by Azure AD.

When a user authenticates using single sign-on, HMP takes the User Principal Name (UPN) from the token that it receives from the identity provider and creates a user session for the HMP user with that associated UPN. For AD FS, the Relying Party Trust that HMP is configured to use should pass through the UPN as a claim.

To integrate Haivision Media Platform with an SSO environment:

1. On the Directory Services pane, verify that the **Directory Service** button is toggled to **On**.
2. Scroll down the Directory Services pane and toggle the Single Sign-On button to **On**.
3. Select the Sign-In Protocol for your system, either: OAuth2, WS-Fed, or SAML2.

 **Note**

- Azure AD and AD FS 2.0+ support authentication using WS-Fed and SAML2.
- Azure AD and AD FS 3.0+ (Windows Server 2012 R2) support authentication using OAuth2.

An example OAuth2 screenshot is shown below:

4. Enter values in the remaining fields. See [Single Sign-On \(SSO\) Settings](#).
5. Click **Save Settings** to save the connection.

Single Sign-On (SSO) Settings

The following table lists the Single Sign-On (SSO) settings.

Setting	Description	AD FS-specific	Azure AD-specific
Sign-In Protocol	The Sign-In Protocol for your system, either OAuth2, WS-Fed, or SAML2	—	—
Server Address	The address of the identity provider, either a partial URL or an IP address/host name.	For AD FS, just the host name is sufficient.	For Azure AD, it is generally most convenient to enter your application's sign-on endpoint without the protocol part of the URL, which should be saved for the next field, Endpoint URL Path. For example: <code>https://login.microsoftonline.com/514a94b9-6a5b-4f0b-96aa-63dced118308</code>
Endpoint URL Path	The location on the identity provider's Web server that HMP should redirect unauthenticated browsers to in order to sign in. The Server Address and Endpoint URL Path are combined by HMP to get the full Web address of the sign-in endpoint. For OAuth2, the Endpoint URL Path should not include the authorize or token portions of the URL, as those are defined in the settings below.	If this is empty, HMP assumes that the default AD FS endpoint should be used for the chosen Sign-In Protocol. <ul style="list-style-type: none"> For OAuth2, this is <code>/adfs/oauth2</code> For WS-Fed or SAML2, this is <code>/adfs/ls</code> 	When using Azure AD, set this to the part of the sign-on endpoint that was omitted in the Server Address field. <ul style="list-style-type: none"> For OAuth2, <code>/oauth2</code> For WS-Fed, <code>/wsfed</code> For SAML2, <code>/saml2</code>
Sign-Out URL	If defined, when logging out of HMP, the user is redirected to this SSO logout page.	—	—
Relying Party Identifier	A URI that HMP passes to the identity provider that lets HMP select which configuration should be used to authenticate.	For AD FS, this value identifies the Relying Party Trust. On the Windows Server, this can be found under Administrative Tools in AD FS Management under AD FS → Trust Relationships → Relying Party Trusts. The value that should be configured will be in the "Identifier" column for whichever Relying Party Trust should be used.	For Azure AD, this value identifies the Application. On the AD Application's Configure tab, this is the App ID URI value under the Single Sign-On section. <div style="border: 1px solid #ffc107; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>If the App ID URI value is not a valid URI, add a <code>spn:</code> prefix to the value.</p> </div>

Setting	Description	AD FS-specific	Azure AD-specific
Identity Metadata URL	When HMP's authentication service starts, it loads the Token Signing Certificate automatically from the Identity Metadata URL. Single Sign-On configuration requires either the Identity Metadata URL or Token Signing Certificate field to be configured. If both are configured, HMP uses the specified Token Signing Certificate and ignores the Identity Metadata URL. If the Sign-In Protocol is WS-Fed or SAML2, the Identity Metadata URL should be the identity provider's Federation Metadata document.	<p>For AD FS, an example value is: <code>https://adfstest.local/FederationMetadata/2007-06/FederationMetadata.xml</code></p> <p>The default endpoint on AD FS is <code>/FederationMetadata/2007-06/FederationMetadata.xml</code></p> <div style="border: 1px solid green; padding: 5px;"> <p>Tip</p> <p>You can check what Federation Metadata endpoint is currently set to on Windows Server's Administrative Tools > AD FS Management under AD FS > Service > Endpoints.</p> </div>	<p>For Azure AD, an example Federation Metadata URL is: <code>https://login.microsoftonline.com/514a94b9-6a5b-4f0b-96aa-63dced118308/federationmetadata/2007-06/federationmetadata.xml</code></p> <div style="border: 1px solid green; padding: 5px;"> <p>Tip</p> <p>You can find this by going to your Application on Azure AD and selecting View Endpoints on the bottom of the browser window. The URL is labeled "FEDERATION METADATA DOCUMENT".</p> </div> <p>When the Sign-In Protocol is OAuth2, the Identity Metadata URL should be an OpenID Provider Metadata URL, which is currently available for Azure AD but not AD FS (as of 3.0). An example URL is: <code>https://login.microsoftonline.com/514a94b96a5b4f0b-96aa63dced118308/v2.0/.wellknown/openid-configuration</code></p>
UPN Claim Identity	<p>For default usecases, set the value to <code>upn</code>. This value may be modified to support a claim with another name or a standard property string.</p> <div style="border: 1px solid green; padding: 5px;"> <p>Tip</p> <p>If your SSO login fails, monitor <code>calypso.log</code> for a message such as "Provided UPN field is invalid" and enter the valid string into this field.</p> </div>	—	—

Setting	Description	AD FS-specific	Azure AD-specific
Token Signing Certificate	HMP needs to know the Token Signing Certificate used by the identity provider to verify that any tokens that it receives after a successful sign-in have not been tampered with.	When using AD FS with the Sign-In Protocol set to WS-Fed or SAML2, the Identity Metadata URL setting can be set to the AD FS Federation Metadata endpoint. In this case, the Token Signing Certificate is fetched automatically so this value does not need to be configured. For OAuth2, AD FS on Windows Server 2012 R2 does not currently have an OpenID Provider Metadata endpoint, so the Token Signing Certificate has to be configured	With Azure AD, HMP also fetches Token Signing Certificate automatically from the Identity Metadata URL, so this value does not need to be configured.
Decryption Key	(SAML2 only) The Decryption Key is used to decrypt an encrypted assertion response after a successful sign-in. This setting is optional, as the assertion response may not be encrypted at all depending on the configuration of the identity provider.	With AD FS, the SAML2 assertion response can be encrypted by setting a certificate under Encryption settings for the Relying Party Trust that HMP uses. The Decryption Key should be the HMP private key associated with the certificate that was set. The WS-Fed token can also be encrypted, although HMP does not currently support decrypting it.	No decryption key is required when using SAML2 for Azure AD.
Client ID	(OAuth2 only) When using OAuth2, HMP must have a Client ID with an associated Redirect URI registered on the identity provider. If it does not, or the configured Redirect URI does not match the value that the Client ID was registered with, all Single Sign-On logins will fail.	With AD FS, you can see all of the Client IDs that are currently registered by running the <code>Get-AdfsClient</code> PowerShell cmdlet. The <code>ClientId</code> and <code>RedirectUri</code> fields of the correct client should be set as the values for the Client ID and Redirect URI fields on HMP.	The Client ID can be retrieved from Azure AD by navigating to the Configure tab for the OAuth2 Application and copying the value for Client ID under Properties.
Client Secret	(OAuth2 only) Client Secret is an optional key that HMP can use to get authorized by the identity provider to request access tokens for users.	No client secret is required when using OAuth2 for AD FS.	Client secrets are used by Azure AD. On Azure AD, Client Secrets are simply called keys and can be generated on the application's "Configure" page. Under keys, select a duration for the key to be valid, then click Save on the bottom of the browser window and copy the key value that appears. This is the Client Secret for the application.

Setting	Description	AD FS-specific	Azure AD-specific
Redirect URI	(OAuth2 only) This is the URL that the user should be taken to after authenticating using Single Sign-On. In general, this should be HMP's SSO callback URL, which is <code>https://calypso.local/sso/callback</code> (replacing <code>calypso.local</code> with your HMP's real IP/host name). This field is not used for WS-Fed or SAML2 because the redirect is completely configured on the server side of the identity provider.	—	—
Token Endpoint	(OAuth2 only) Defines the token endpoint. Can be an absolute URL or relative to the server address+endpoint URL path. If not defined, and an OIDC metadata endpoint is configured in the Identity Metadata URL, HMP uses the token endpoint defined in the metadata response. If neither this field nor the Identity Metadata URL is defined, <code>/token</code> path is assumed.	—	—
Authorization Endpoint	(OAuth2 only) Defines the authorization endpoint. Can be an absolute URL or relative to the server address+endpoint URL path. If not defined, and an OIDC metadata endpoint is configured in the Identity Metadata URL, HMP uses the authorization endpoint defined in the metadata response. If neither this field nor the Identity Metadata URL is defined, <code>/authorization</code> path is assumed.	—	—
User Info Endpoint	(OAuth2 only) Defines the user info endpoint. Must be an absolute URL. If not defined, and an OIDC metadata endpoint is configured in the Identity Metadata URL, HMP uses the user info endpoint defined in the metadata response.	—	—


Licensing Your HMP

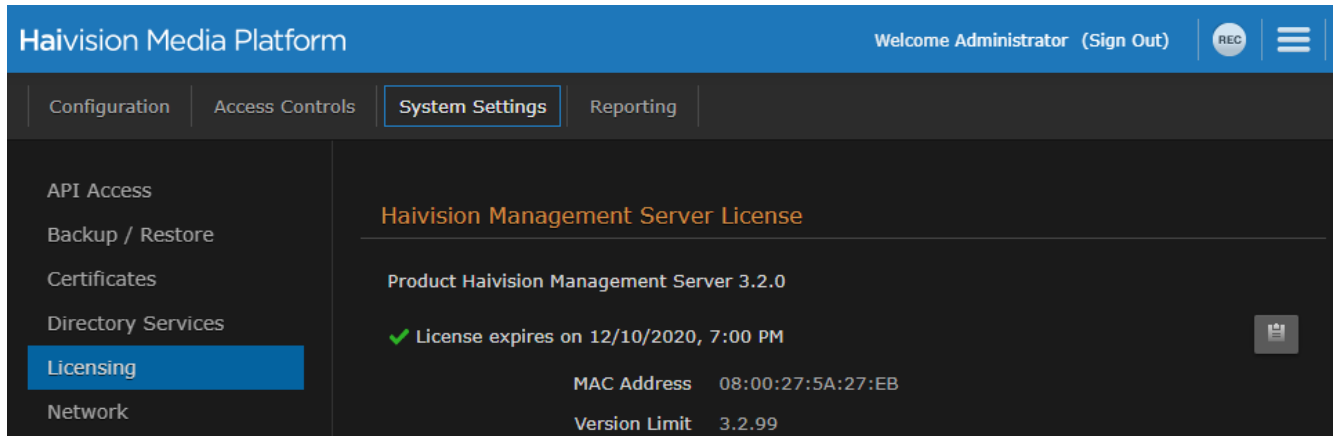
This section provides instructions to update your Haivision Media Platform license from the Web interface. For major releases or when purchasing licensed options, you need to obtain a valid license key from Haivision Technical Support and apply it before updating. For example, KLV, EPG, Network Storage, and Multicast Agent support are licensed options.

Note

- Any update (other than a maintenance release, such as version 3.x.x) requires a new license.
- Haivision Media Platform is available in product editions to suit different applications. For more information, see [Product Editions](#).

To update your license:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **System Settings** on the toolbar and then click **Licensing** on the sidebar. The License pane opens, showing the installed license, including its expiration date, product edition, and licensed features.



Note

- With VM installations, the display shows the Instance UUID and CPU ID (if available); Whereas with regular (non-VM) installations, those two fields are not displayed.
- With HA installations, license details of the secondary servers also appear.

3. To request a license for your product:
 - a. Log in to the [Haivision Support Portal](https://support.haivision.com) (https://support.haivision.com).
 - b. After logging in, click **License Requests**.
 - c. Click the **New** button.
 - d. Select the appropriate device type and click the **Next** button.
 - e. Fill in the form with the appropriate information, and click **Save**. Your license request is submitted and you will be contacted by a Haivision representative shortly with a license key for your product.
4. After you receive the license file from Haivision, drag it into the HMP License Update drag area or click **Choose a file**.

Note

With HA installations, ensure that all nodes are online and available before installing a new license.

- Click **Upload** to upload the license to HMP.
The features of your license appears in the License Features section.

Haivision Management Server License

Product Haivision Management Server 3.2.0

✔ License expires on 12/10/2020, 7:00 PM 📄

MAC Address	08:00:27:5A:27:EB
Version Limit	3.2.99


License Features

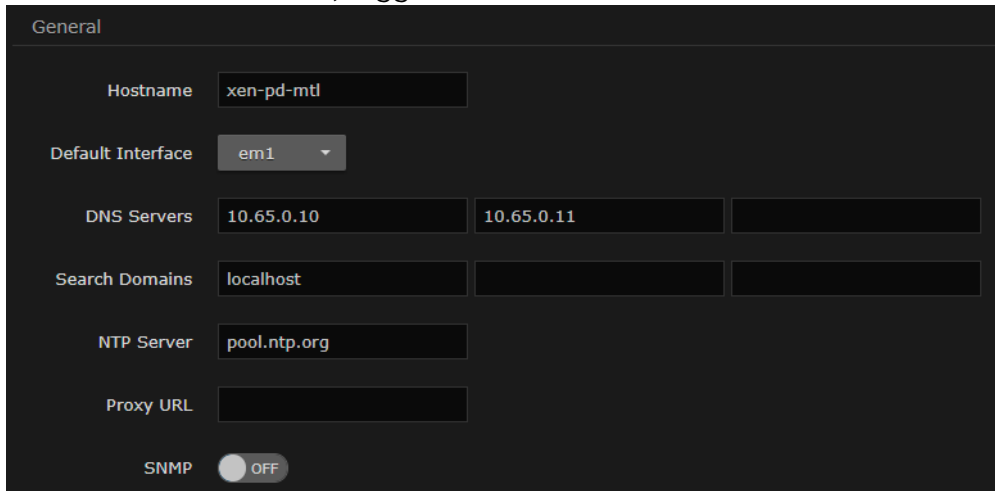
	Edition	Enterprise
Maximum Concurrent Users		2500
Maximum Concurrent Recordings		5
Maximum Sources		Unlimited
Output Bandwidth Limit		9999 Mbps
Input Bandwidth Limit		9999 Mbps
	IPTV	Enabled
	EPG	Enabled
	KLV	Disabled
Multi-site eCDN		Enabled
Multicast Agent		Enabled
Play Mobile Contribution		Enabled
Remote Storage		Enabled
Single Sign-On (SSO)		Enabled
Video On Demand (VOD)		Enabled

Configuring Network Settings


When setting up Haivision Media Platform, you need to configure the network settings. This includes general settings, such as specifying the server hostname, IP address, subnet mask, and DNS servers, as well as advanced settings, such as setting up multiple network interfaces, NIC bonding, link negotiation settings, and static routes.

To configure the network settings:

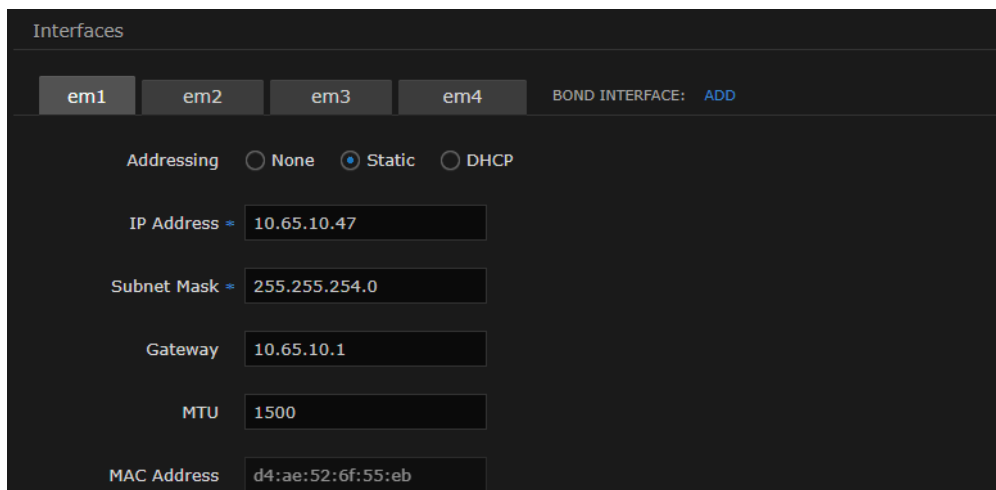
1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **System Settings** on the toolbar and then click **Network** on the sidebar. The Network Configuration pane opens.
3. Fill in the General section. For details, see [Network Settings](#).
 - To enable SNMP alerts, toggle the SNMP button to **On** and enter the SNMP-specific fields.



4. Under Interfaces, select the tab for the first interface, if not already selected.
5. Fill in the required fields. For details, see [Network Settings](#).
 - In the Addressing field, select either DHCP or Static to enable or disable the Dynamic Host Configuration Protocol for the interface.

 **Note**

- When DHCP is enabled, HMP receives an IP Address from a DHCP server on the network it is connected. When it is disabled, you must manually enter the appliance’s IP Address and Netmask.
- If your network uses addresses within the 172.16.0.0/12 range, please contact [Haivision Support](#) for additional configuration steps.



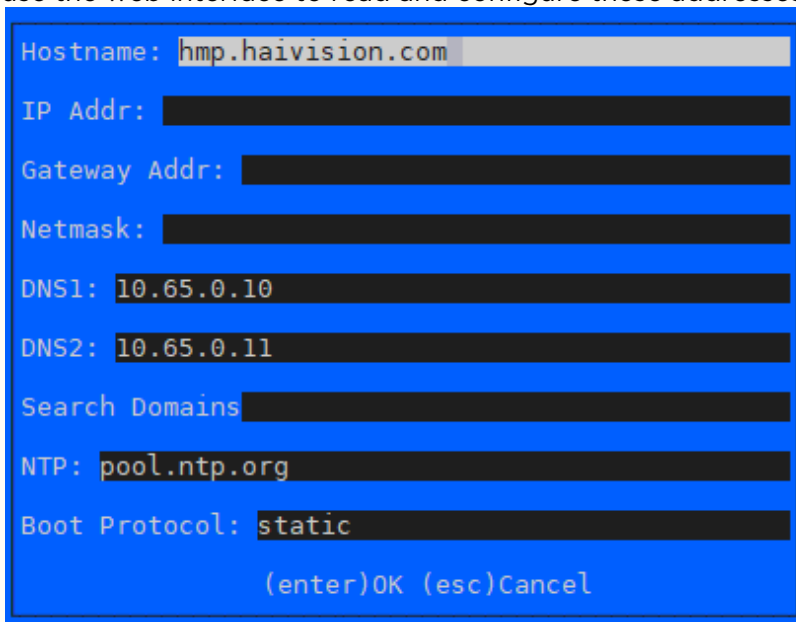
6. To configure multiple network interfaces, select the next interface (e.g., em2) tab and repeat the configuration.
7. To add a bond interface, click **Add** and fill in the fields, including the Bonding Mode.

Tip

Bond interfaces provide a method for aggregating multiple network interfaces into a single logical bonded interface. The goal is to increase throughput and to ensure redundancy in case one of the links should fail. See the "Bond Interface" in [Network Settings](#).

Note

When a bonded interface is used, various address fields in the Console UI Network Settings screen appear blank. This is a known issue and will be corrected in a future release. Please use the web interface to read and configure these addresses.



8. To add one or more static routes, click **+** button under Static Routes and fill in the fields.
9. Click **Save Settings**.
10. Click **Reboot** and click **Confirm** for the new network settings to take effect.

A dialog appears informing you when the reboot is complete.

Topics Discussed

- [Network Settings](#)

Network Settings



The following table lists the configurable Haivision Media Platform Network settings.

Note

Please contact your Network Administrator if you are unsure what to put in any of these fields or if you are unsure whether the setting is required on your network.

General Interfaces Static Routes

General

Setting	Description
Hostname	The hostname to be assigned to HMP. This is a FQDN (Fully Qualified Domain Name); for example, myserver.mycompany.com.
Default Interface	<p>The default Ethernet interface: Select an available interface, such as eth0, eth1, em1, or em2.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>Network Interface names for Ethernet interfaces may vary, such as eth0/eth1/... or em1/em2/.... "None" or Blank indicates that the default interface is not set.</p> </div>
DNS Servers	(Optional) The IPv4 addresses of the Domain Name Servers.
Search Domains	(Optional) The search strings to use when attempting to resolve domain names.
NTP Server	(Optional) If IP address or FQDN of the Network Time Protocol (NTP) server.
Proxy URL	(Optional) If your network routes web traffic through a proxy server, enter the proxy server address or port. If required, you may also enter a username and password in the URL as well. For example: <code>user:password@proxyserver:proxyport</code>
SNMP	<p>To enable SNMP (Simple Network Management Protocol) alerts for out-of-band monitoring, toggle this button to On. This starts the SNMP server to query for OS information, such as CPU usage. SNMP alerts are typically used by IT administrators to monitor system health. See Using SNMP with HMP for more details.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Tip</p> <p>There are no HMP-specific MIBs.</p> </div>

Setting	Description
Read-Only Community	(SNMP must be enabled) Enter the SNMP community string associated with the SNMP Trap Server. This is the string to use when sending a trap to an SNMP Trap server. For example: "Haivision Media Platform".
SNMP Trap Servers	(SNMP must be enabled) Enter the IP address or FQDN of the SNMP server to send SNMP Traps to.

General Interfaces Static Routes

Interfaces

If multiple network interfaces are available on your HMP, the settings for each interface are organized within their own tab.

Setting	Description
Bond Interface	Bonding enables an administrator to use more than one physical network port as a single connection. This can be used to increase performance or redundancy of a server. See the Bonding Mode entry in this table.
Addressing	Choose whether the interface uses a static or dynamic IP address:
IP Address	<p>The IP Address for the interface. This is a unique IPv4 address that identifies the unit in the IP network.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>Note</p> <ul style="list-style-type: none"> If DHCP is disabled, you may enter an IP address in dotted-decimal format (xxx.xxx.xxx.xxx). If your network uses addresses within the 172.16.0.0/12 range, please contact Haivision Support for additional configuration steps. </div>
Subnet Mask	<p>The IPv4 network mask for the interface. This is a 32-bit mask used to divide an IP address into subnets and specify the network's available hosts.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>Note</p> <p>If DHCP is disabled, you may enter a Network Mask in dotted-decimal format (e.g., 255.255.0.0).</p> </div>
Gateway	<p>The IPv4 default route to be assigned to the interface. This is the gateway that is used when no other route matches. This address must be reachable on your local subnet.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>Note</p> <p>If DHCP is disabled, you may enter a gateway address in dotted-decimal format.</p> </div>
MTU	(Maximum Transmission Unit) Specifies the maximum allowed size of IP packets for the outgoing data stream. 228..1500
MAC Address	(Read-only) The Media Access Control address assigned to the interface. This is the physical address of the network interface and cannot be changed.

Setting	Description
Link	Select the link negotiation settings for the interface, either Auto or Manual. If you select Manual, you can select the Speed (10, 100, or 1000) and Duplex setting (Full or Half).
Bonding Mode	<p>(Bond Interface only) Modes for the Linux bonding driver determine the way in which traffic sent out of the bonded interface is actually dispersed over the real interfaces. Modes 0, 1, and 2 are by far the most commonly used among them.</p> <ul style="list-style-type: none"> • Round Robin Sequential: Transmits packets in first available network interface (NIC) slave through the last. This mode provides load balancing and fault tolerance. • Active Backup: Only one NIC slave in the bond is active at a time. A different slave becomes active only when the active slave fails. This mode provides fault tolerance • XOR Sequential: Transmits based on XOR formula. (Source MAC address is XOR'd with destination MAC address). This mode selects the same NIC slave for each destination MAC address and provides load balancing and fault tolerance. • Broadcast - Fault Tolerance: Transmits network packets on all slave interfaces. This mode is least used (only for specific purpose) and provides only fault tolerance. • IEEE 802.3ad Dynamic Link Aggregation: Creates aggregation groups that share the same speed and duplex settings. Utilizes all slave network interfaces in the active aggregator group according to the 802.3ad specification. This mode is similar to the XOR mode above and supports the same balancing policies. The link is set up dynamically between two LACP-supporting peers. • (Adaptive) Transmit Load Balancing (TLB): The outgoing traffic is distributed according to the current load and queue on each slave interface. Incoming traffic is received by one currently designated slave network interface. If this receiving slave fails, another slave takes over the MAC address of the failed receiving slave. • (Adaptive) Active Load Balancing (ALB): This includes balance-tlb + receive load balancing (rlb) for IPV4 traffic. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the server on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different clients use different hardware addresses for the server.
Slave Interfaces	(Bond Interface only) Check this checkbox to select the slave interface(s) to allow the bond interface be the master.

General Interfaces Static Routes

Static Routes

Setting	Description
+ Route	<p>Click and fill in the values to add one or more static routes.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>A static route cannot be created with a Subnet Mask of either 0.0.0.0 or 255.255.255.255.</p> </div>


Managing Network Storage

Network Storage is a licensed option that allows you to move video storage from your HMP server to Network-Attached Storage (NAS) through a Network File System (NFS) connection.

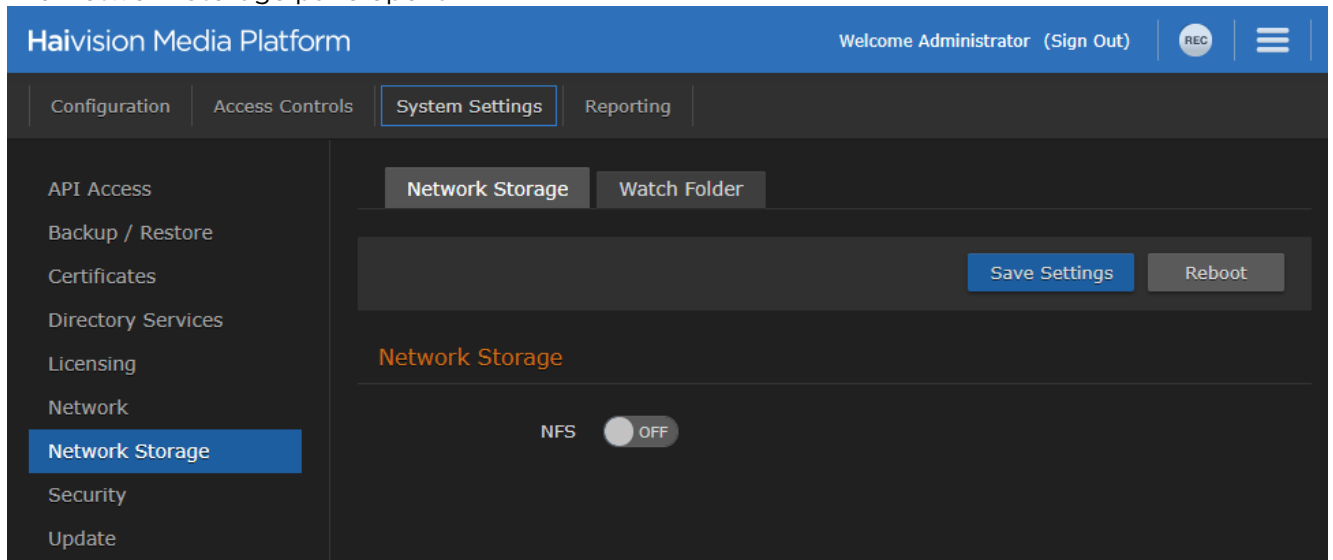
Note

- For information on the Network Storage licensed option, please contact Haivision Sales.
- The NFS server must be configured on your host before configuring network storage on Haivision Media Platform.

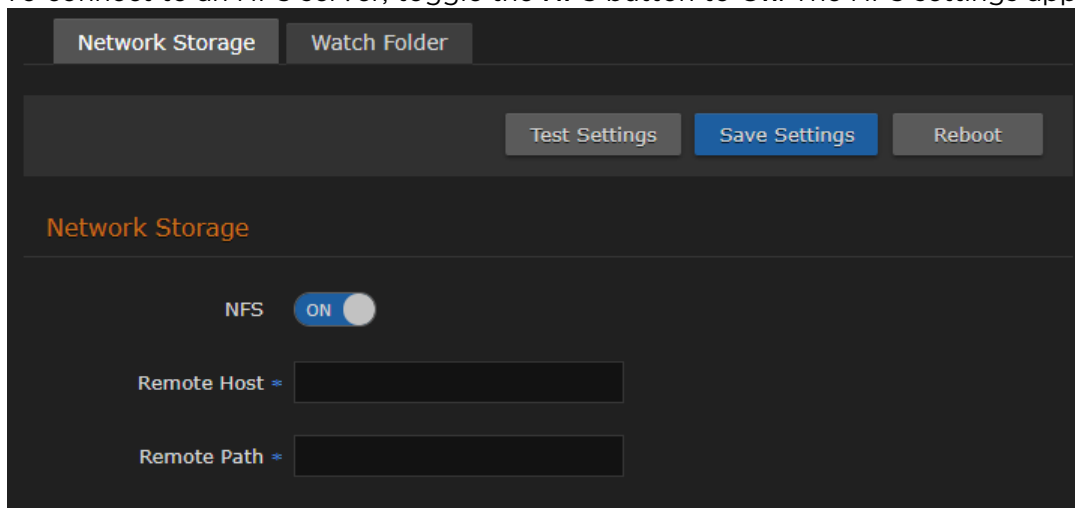
To configure network storage:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **System Settings** on the toolbar and then click **Network Storage** on the sidebar.

The Network Storage pane opens.



3. To connect to an NFS server, toggle the **NFS** button to **On**. The NFS settings appear:



4. Enter the remote host IP address and path.
5. To test the connection from HMP to the defined NFS server, click **Test Settings**.
6. Click **Save Settings** to save the connection.

- Click **Reboot** and click **Confirm** to restart the HMP server.
A dialog appears informing you when the reboot is complete.
- After the reboot, click **Migrate** to copy your videos and non-video data to the NFS server.
The progress bar shows the progress of the migration. Your videos and non-video data are now stored on the defined NFS server.

Topics Discussed

- [Configuring Watch Folders](#)
- [Formatting XML Data to Import into HMP with Media Files](#)
- [Importing Custom EPG Data into HMP](#)

Configuring Watch Folders

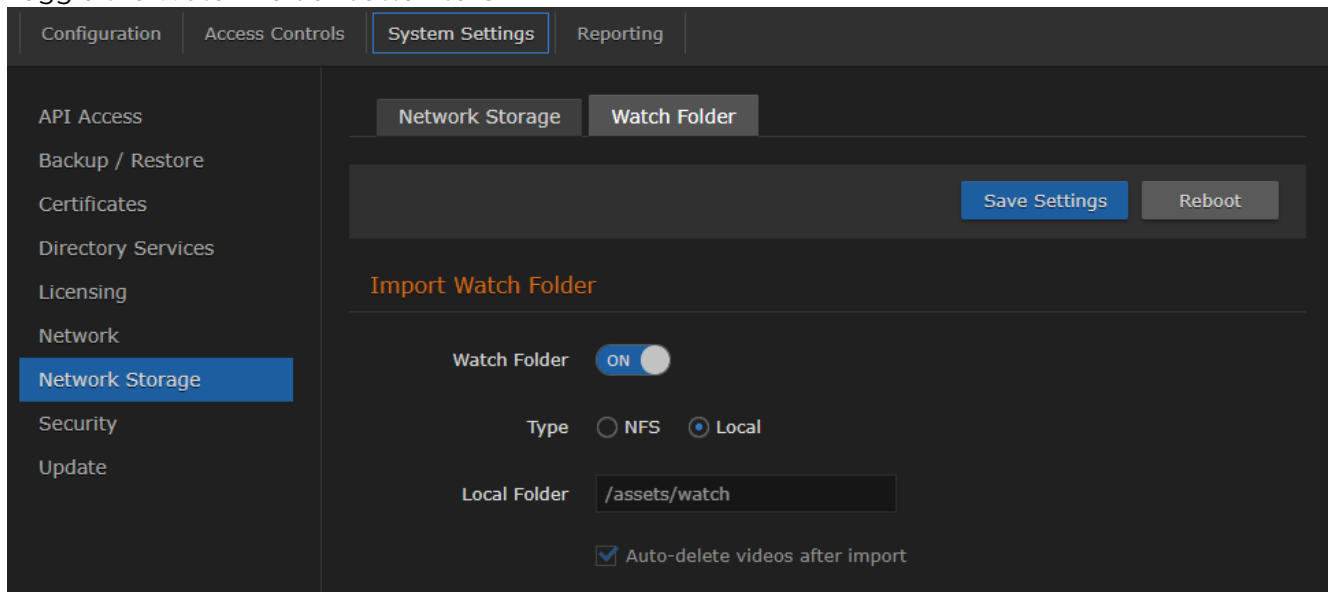
Administrators can also create, edit, and delete a watched folder (enabled either as an Network File System (NFS) or Local folder) that can be configured for permission-based writing (by HMP users). HMP watch folders also support import/ingest of XML sidecar metadata for media assets, and XMLTV files with custom EPG data. The watch folder is a single ingest folder, and HMP processes it recursively.

Note

Files that have been synced from a watch folder do not reappear if they have expired or been removed from HMP (or otherwise made offline).

To configure a watch folder:

- On the Network Storage pane, click the **Watch Folder** tab.
- Toggle the Watch Folder button to **On**.



- Select the folder type. The watch folder can either be on a separate NFS mount or local to the `/assets` directory (which may itself be on a physical HMP drive or on a separate NFS volume).
If you choose NFS, provide a remote host address and path.
- Click **Save Settings** to save the connection.
- Click **Reboot** and click **Confirm** to restart the HMP server.

A dialog appears informing you when the reboot is complete.

Tip

To automatically import from a Makito X with Storage:

1. The Makito X export manager creates a folder named "recordings" on the Makito X-configured external storage (NFS or FTP).
2. On HMP, configure the Watch Folder settings to point to this recordings folder to automatically import videos.

Formatting XML Data to Import into HMP with Media Files

Haivision Media Platform supports importing HMP XML files while editing existing assets or assets that are in the process of being imported. Metadata imported from the HMP XML file completely overwrites the existing asset metadata.

The following table describes the handling of various HMP XML elements. Elements that are described as optional may be left out of the XML file and the corresponding record on the asset is left as is.

Element	Required	Notes
id	Ignored	The original asset UUID is always preserved.
title	Optional	When no title is specified, the video filename is used.
description	Optional	Plain text description with all HTML tags removed.
htmlDescription	Optional	The description with HTML tags and embedded images.
ctime	Optional	The source creation time in Unix timestamp (seconds).
mtime	Ignored	The source's last modified time in Unix timestamp (seconds). Importing an HMP XML file updates the asset's mtime to the present.
duration	Ignored	Duration of the asset is calculated by HMP.
metadata	Optional	If missing, metadata and HotMarks on the asset are left as is. If included, all metadata including HotMarks is overwritten with the new data.
media	Ignored	HMP already has internal records of the asset's tracks and posters.

Categories

Category values from an HMP XML file are added to an asset's metadata even when that category does not exist on the importing system.

The HMP system from which the HMP XML file was exported may not have the same metadata and metadata values as the system to which it is imported. After importing metadata values to a system that does not have the corresponding metadata, the following behaviors can be observed:

- The exported system's metadata and values do *not* show up on imported asset's Edit Metadata pane.
- The exported system's metadata values show up on the REST API at `/assets/:id/metadata`.
- Editing the imported asset's metadata values through the Web interface works and does not cause the imported XML metadata values to be deleted.

- When metadata with the same label as the metadata from the imported XML is created, the metadata and the selected values become visible on the imported asset's Edit Metadata pane.
- All metadata values from the imported XML are preserved even when "Custom Values" or "Multiple Values" is not enabled for metadata with the same name, and these values are still preserved when editing values from the Edit Metadata Pane.

Other Metadata

HMP XML import does not check whether other metadata makes valid references on the new system.

- `calypso:recorded_from_session` - If the session does not exist, it no longer shows up as a related asset on any session.
- `calypso:creator` - If the creator does not exist, it does not show up under the "Mine" Browse Content filter for anyone.
- `calypso:expiration_timestamp`
- `calypso:recordGeaddress`
- `calypso:recordGeolocation`

HotMarks

If the HotMark timestamp described in HMP XML is greater than the duration of the asset to which it is imported, an error is returned and the XML import fails. However, if the asset does not have a duration, the XML import succeeds. This can happen when the asset itself is still being imported and no duration can be calculated yet. If the resulting imported asset has a duration less than the HotMark, then that HotMark timestamp is not visible on the player, but appears in the `/assets/:id/hotmarks` API.

Example HMP XML File

```
<asset xmlns="http://xml.haivision.com/calypso" version="1.0">
  <id>a38d140c-2f21-4d14-a1f4-4bee069d5014</id>
  <title>Food TV</title>
  <description>Rachel Ray and a refrigerator</description>
  <ctime>1391542482</ctime>
  <mtime>1391542540</mtime>
  <duration>10868</duration>
  <metadata>
    <entry>
      <name>calypso:creator</name>
      <field>
        <type>STRING</type>
        <value>haiadmin</value>
      </field>
    </entry>
    <entry>
      <name>calypso:recorded_from_session</name>
      <field>
        <type>STRING</type>
        <value>a849de4a-f588-4904-b119-0ff53fda8cae</value>
      </field>
    </entry>
    <entry>
      <name>calypso:recordGeaddress</name>
      <field>
        <type>STRING</type>
        <value>4445 Rue Garand:Montréal:QC:H4R2H9:Saint-Laurent:Rue Garand:4445:Canada</value>
      </field>
    </entry>
  </metadata>
</asset>
```



```

<entry>
  <name>calypso:recordGeolocation</name>
  <field>
    <type>STRING</type>
    <value>+45.4913235,-73.7214226</value>
  </field>
</entry>
<entry>
  <name>calypso:category:keywords</name>
  <field>
    <type>STRING</type>
    <value>Rachel Ray</value>
  </field>
  <field>
    <type>STRING</type>
    <value>Food</value>
  </field>
  <field>
    <type>STRING</type>
    <value>Refrigerator</value>
  </field>
</entry>
<entry>
  <name>calypso:htmlDescription</name>
  <field>
    <type>STRING</type>
    <value>&lt;b>Test</b>&lt;/b>&lt;div>&lt;img src= "data:image/jpeg;base64,/9j/4Q5.....</
value>
  </field>
</entry>
</metadata>
<media>
  <movie>
    <index>0</index>
    <name>a38d140c-2f21-4d14-a1f4-4bee069d5014-1.mp4</name>
    <format>mp4</format>
  </movie>
  <poster>
    <index>0</index>
    <name>a38d140c-2f21-4d14-a1f4-4bee069d5014.png</name>
    <format>PNG</format>
  </poster>
</media>
</asset>

```

Importing Custom EPG Data into HMP

Haivision Media Platform supports importing XML files containing custom EPG data in XMLTV format.

When the watch folder feature is enabled, HMP automatically creates an `/xmltv` directory within `/watch`. When you upload a single `.xml` file containing the XMLTV data or a `.tar.gz` archive containing multiple `.xml` files to the `/watch/xmltv` folder, HMP detects the upload, waits 20 seconds for it to complete, and then ingests the files. After processing, the custom EPG channels are available to be

scheduled in a source (added to the existing channel list, if any), as shown below:

The screenshot shows the 'Add Source' configuration interface. The 'Name' field is set to 'Source - 8/28/2019, 2:49 PM'. The 'Receiver' is set to 'Haivision Management Server (10.65.10.47)'. The 'Type' is set to 'UDP'. The 'IP Address' and 'Port' fields are empty. The 'Multicast Stream' checkbox is checked, 'View Direct' is unchecked, and 'IPTV Channel' is checked. The 'EPG' toggle is set to 'ON'. The 'Schedule' dropdown menu is open, displaying a list of channels: 4Music (selected), 4Seven, 5 Star, SUSA, A&E, A&E (West), ABCF Dupe, AETV Dupe, AMC, and APL Dupe.

⚠ Note

Both read and write permissions must be set on any files uploaded to the `/xmltv` folder, or the import fails. After successfully imported, any uploaded files are automatically erased.

Example XMLTV File


```
<tv>
  <channel id="215eaf21-b721-4188-9f63-40d911fb7557">
    <display-name>Haivision Shark Fest</display-name>
    <display-name>HSF</display-name>
  </channel>
  <programme channel="215eaf21-b721-4188-9f63-40d911fb7557" start="2017072900000 +0000"
  stop="20170729003000 +0000">
    <title lang="en">Hammer Head Shark Fest</title>
    <desc lang="en">Hammer head wears a t-shirt</desc>
    <rating system="VCHIP">TVMA</rating>
  </programme>
  <programme channel="215eaf21-b721-4188-9f63-40d911fb7557" start="20170729003000 +0000"
  stop="20170729020000 +0000">
    <title lang="en">Tiger Shark</title>
    <desc lang="en"> Tiger Shark fights off a dolphin</desc>
  </programme>
  <programme channel="215eaf21-b721-4188-9f63-40d911fb7557" start="20170729020000 +0000"
  stop="20170729030000 +0000">
    <title lang="en">Sharknado</title>
    <desc lang="en">Shark documentary in tornado of souls</desc>
    <rating system="VCHIP">TVMA</rating>
  </programme>
</tv>
```

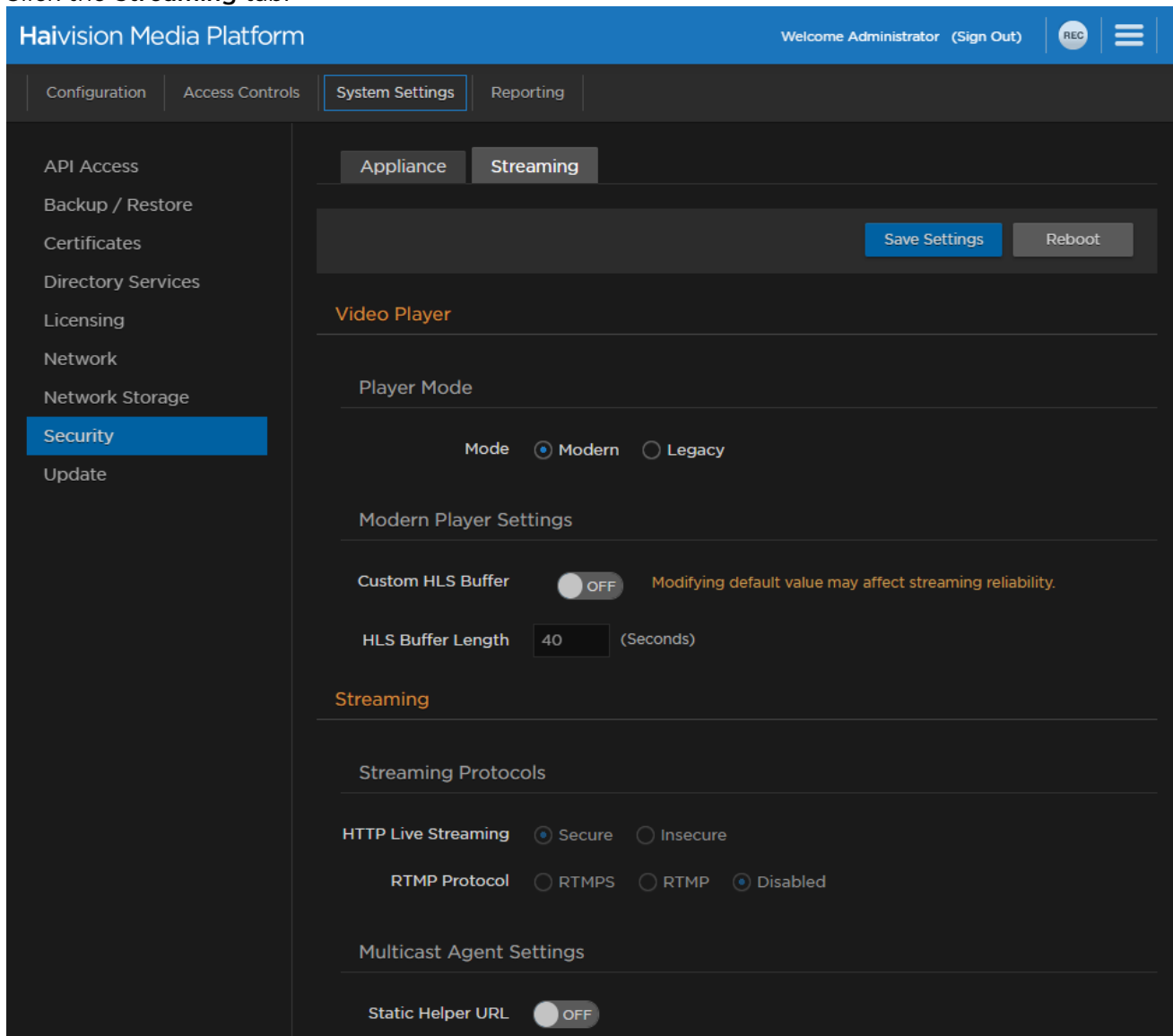
A detailed description of the XMLTV format is available at <http://wiki.xmltv.org/index.php/XMLTVFormat>.

Managing Security

When setting up Haivision Media Platform, you may configure a range of security settings. HMP supports encrypted streaming from the appliance to the desktop. From the Streaming pane, you can also set desktop browser playback to either a native HTML5 player (via HLS) or a Flash-based player.

To configure the video player and streaming options:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **System Settings** on the toolbar and then click **Security** on the sidebar.
3. Click the **Streaming** tab.



4. To switch the browser player mode between the HTML5 and Flash-based players, select either Modern or Legacy. Depending on your selection, customizable buffer settings appear. See the Video Player settings under **Security Settings** for more details.

5. For the Legacy player only, select the Streaming Protocols. See the Streaming Protocols entry in [Security Settings](#).
6. (Optional) To specify a fixed hostname for the multicast agent download, toggle the Static Helper URL button to **On**. See Multicast Agent Settings under [Security Settings](#).
7. Click **Save Settings**.
8. Click **Reboot** and click **Confirm** for the new settings to take effect.

A dialog appears informing you when the reboot is complete.

Configuring Appliance Security

From the Appliance pane, you may configure the following additional system security settings:

- FIPS compliance

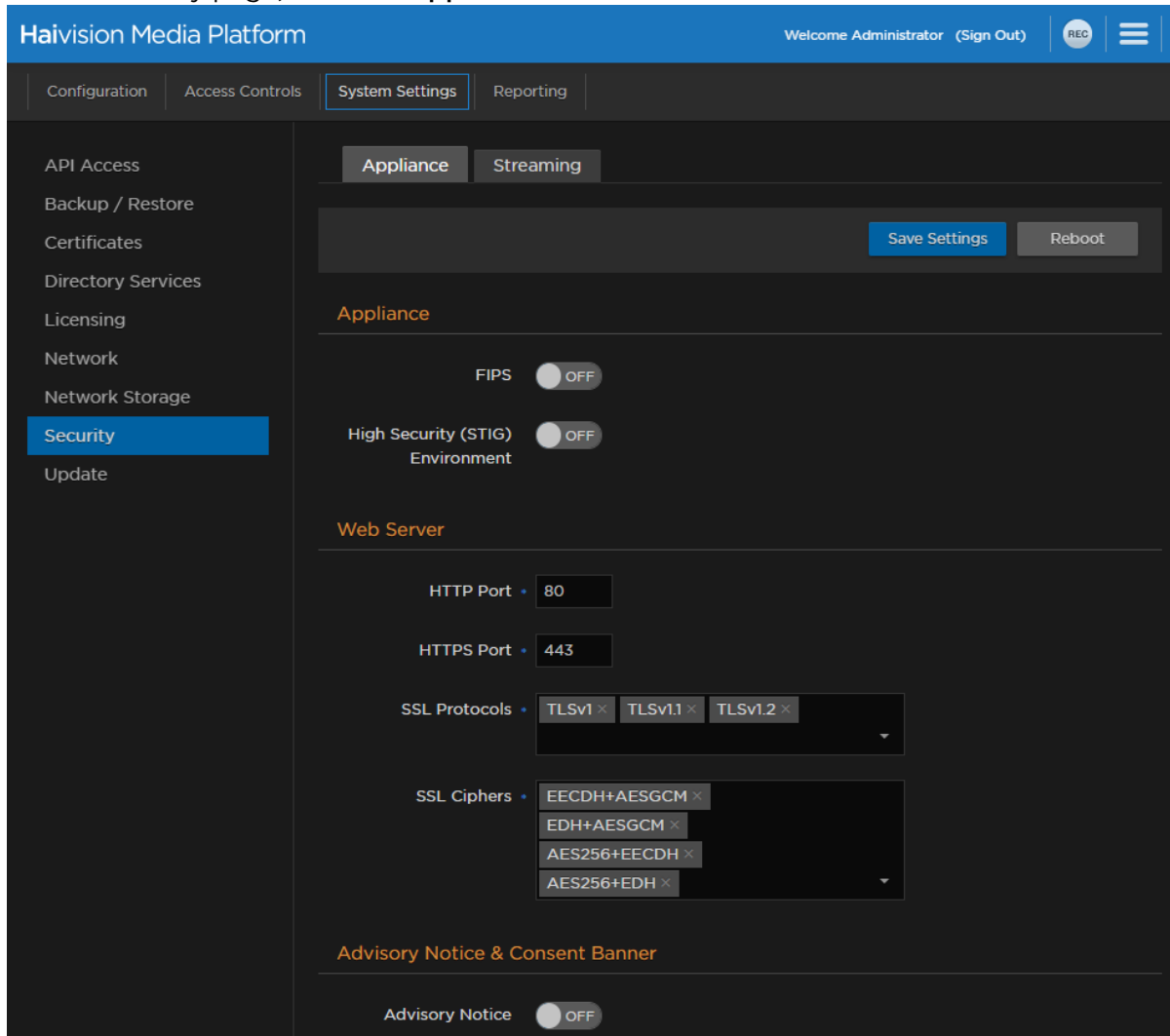
 **Note**

Streams from the source to Haivision Media Platform may be unencrypted, depending on whether you are using UDP or SRT.

- High Security (STIG) Environment hardening settings
- Web Server security and policy settings
- Advisory Notice & Consent Banner

To configure appliance security:

1. On the Security page, click the **Appliance** tab.

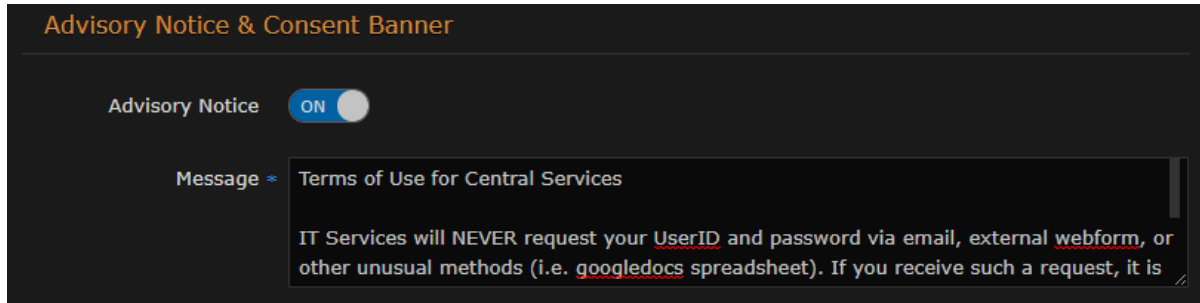


2. Under Appliance:
 - To configure FIPS compliance, toggle the FIPS button to **On**. See the Appliance entry in [Security Settings](#).
 - To enable security hardening features for high-security environments, toggle the High Security (STIG) Environment button to **On**.
3. Under Web Server, to configure security and policy settings, specify the HTTPS or HTTP port, SSL protocols, and SSL cipher values, as required. See the Web Server entry in [Security Settings](#).

⚠ Important

Port number changes take effect immediately and affect ongoing operations using the service at that port.

- Under Advisory Notice & Consent Banner, to configure a banner, toggle Advisory Notice to **On** and enter the desired banner text.



- Click **Save Settings** to save the connection.
- Click **Reboot** and click **Confirm** for the new settings to take effect.

Note

All settings except for those within Web Server require a reboot.

A dialog appears informing you when the reboot is complete.

Security Settings

The following table lists the configurable Haivision Media Platform Security settings.

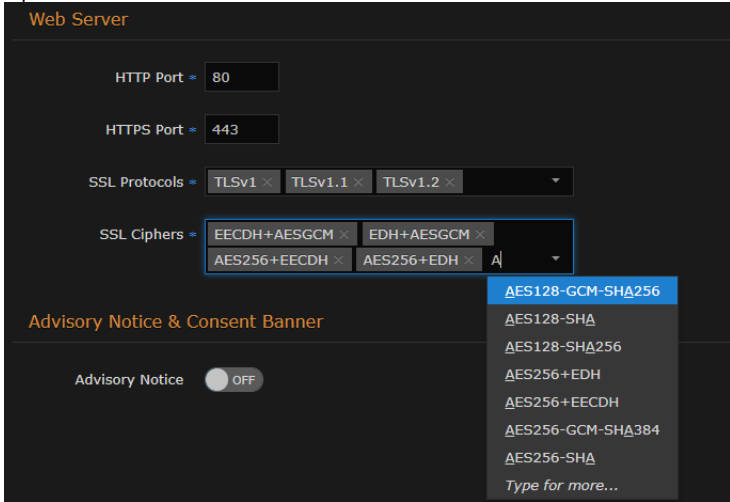
Note

Please contact your Network Administrator if you are unsure what to put in any of these fields or if you are unsure whether the setting is required on your network.

Appliance Streaming

Setting	Description
Appliance	
FIPS	<p>To enable FIPS cryptographic compliance on your system, toggle the FIPS button to On. Enabling FIPS cryptographic compliance applies cryptographic modules accredited under the U.S. Federal Information Processing Standard (FIPS) Publication 140-2.</p> <p>Note</p> <p>To use FIPS mode, the CPU must include support for the RDRAND instruction. As a result, HMP VMware ESXi VMs can only run in FIPS mode on the following physical hardware:</p> <ul style="list-style-type: none"> • AMD desktop and server processors released March 2017 and later. • Intel desktop and server processors utilizing Ivy Bridge (April 2012) or newer microarchitecture.

<p>High Security (STIG) Environment</p>	<p>To enable security hardening features for high-security environments, toggle this button to On. This setting includes:</p> <ul style="list-style-type: none"> • Session timeouts/locks for all interfaces. • Stronger password requirements. • Lock/disable accounts due to multiple authentication failures or expired passwords. • Disabling unnecessary services. <p>These steps are applied when the STIG setting is enabled, and are rolled back/canceled when the STIG setting is disabled.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>This setting complies with National Institute of Standards and Technology (NIST) Special Publication 800-53 (see https://nvd.nist.gov/800-53/ Rev 4).</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Important</p> <ul style="list-style-type: none"> • Only security professionals who understand the cipher support and requirements within their organization should change this setting. • Some of these settings are not supported by Haivision Play Set-Top Box or by Google Chrome. • The default list has been verified for broad acceptance, and should typically only be adjusted to mitigate new and critical vulnerabilities that may occur. </div>
<p>Lock Session After</p>	<p>(High Security (STIG) Environment must be enabled) Enter the inactivity time period (in minutes) before the user's HMP session is locked (on all interfaces: Console UI, SSH, and Web).</p>
<p>Web Server</p>	
<p>HTTP Port HTTPS Port</p>	<p>Configures the Web ports for HMP:</p> <ul style="list-style-type: none"> • HTTP port number (Default = 80) • HTTPS port number (Default = 443) <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Important</p> <p>If you change the HTTP/HTTPS ports, any connected STBs lose connection and need to be redirected to the new port. This can be done manually through the settings on the STB. However, we recommend that you contact Haivision Technical Support if you intend to change port settings and automatically migrate your STBs.</p> </div>
<p>SSL Protocols</p>	<p>To specify which TLS (Transport Layer Security) versions are accepted, select from the drop-down list: TLS v1, TLS v1.1, TLS v1.2.</p>

<p>SSL Ciphers</p>	<p>To specify which SSL Ciphers are accepted, select from the drop-down list or enter the cipher name:</p> 
<p>Advisory Notice & Consent Banner</p>	
<p>Advisory Notice</p>	<p>When enabled, the banner appears when users sign in (Console UI, SSH, and Web interface) and remains on the screen until the user acknowledges the usage conditions and takes explicit actions for further access. The banner is typically an advisory/warning notice to be displayed before the Sign-in page. To enable the banner (as shown in the text box), toggle the Advisory Notice button to On and enter the banner text into the Message text box.</p>

Appliance [Streaming](#)

Setting	Description
<p>Video Player</p>	
<p>Player Mode</p>	<p>To switch desktop browser playback between the HTML5 and Flash-based player, select either:</p> <ul style="list-style-type: none"> • Modern: The Modern player is a native HTML5 player (via HLS) for use in all supported desktop browsers. It supports a Flash fallback mode for older browsers that do not support HTML5 video. The Modern player may require slightly more buffering time than the Legacy player, due to differences in HLS vs. RTMP. Protocol must be set to HLS and HTTP Live Streaming (HLS) must be Secure. New HMP installations default to the Modern player. <div data-bbox="500 1465 1477 1570" style="border: 1px solid #ccc; padding: 5px;"> <p>Note KLV is not supported with the modern player.</p> </div> <ul style="list-style-type: none"> • Legacy: Flash-based player. Systems upgraded from version 2.6 default to the Legacy player. <p>Player Mode is a system-wide setting.</p>
<p>Custom HLS Buffer</p>	<p>(Player Mode must be Modern) To tune the HLS video buffer, toggle the Custom HLS Buffer button to On and enter the desired HLS Buffer Length.</p> <div data-bbox="457 1738 1477 1843" style="border: 1px solid #ccc; padding: 5px;"> <p>Note Modifying the default HLS buffer length may affect streaming reliability.</p> </div>

HLS Buffer Length	(Player Mode must be Modern) Enter the desired buffer length. Range: 1-40 seconds.
Custom RTMP Buffer	(Player Mode must be Legacy) To tune the Flash video buffer to smooth playback, toggle the Custom RTMP Buffer button to On and enter the desired RTMP Buffer Length.
RTMP Buffer Length	(Player Mode must be Legacy) Enter the desired buffer length. Range: 0.5-5 seconds.
Streaming	
HTTP Live Streaming (HLS)	<p>(Only editable when Player Mode is Legacy) Choose whether HMP uses secure (encrypted) or insecure (unencrypted) mode for HLS streaming. Set to Secure by default.</p> <ul style="list-style-type: none"> Secure: Ensures that users cannot stream on a mobile device without a valid security certificate. Insecure: Allows users to stream on a mobile device without a valid security certificate. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>If you select Secure, some mobile devices (notably iPhone/iPad) cannot display the stream unless you have a valid SSL certificate.</p> </div>
RTMP Protocol	<p>(Only editable when Player Mode is Legacy) Choose whether HMP uses a plain or secure streaming protocol:</p> <ul style="list-style-type: none"> RTMPS: Select to enable secured RTMP. RTMPS encryption uses SSL (Secure Sockets Layer) certificates to encrypt the traffic for the Web browser. HMP ships with a self-signed SSL certificate which works with any configured server hostname. However, Web browsers do not consider this to be a trusted certificate because it was not signed by a Certificate Authority. <p>When accessing the Web interface, users see a security warning and may be prompted for authorization each time they try to view a video. Some Web browsers may reject the RTMPS connection completely.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Important</p> <p>Haivision recommends that site administrators install a signed SSL certificate if they plan to use RTMPS streaming. Site administrators should generally contact their Network Administrators for help getting SSL certificates. See Managing Certificates for details.</p> </div> <ul style="list-style-type: none"> RTMP: Select to enable standard RTMP. Disabled: Select to disable RTMP.
Static Helper URL	<p>To specify a fixed hostname for the multicast agent download, toggle the Static Helper URL button to On.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>For multicast streaming, Haivision Helper includes a valid SSL certificate that uses a wildcard name. This option allows organizations to use a static address instead. (This is useful in environments without access to the Internet or a DNS server.)</p> </div> <p>For more information, refer to "Haivision Media Platform Integration" in the Haivision Helper Installation Guide.</p>

Peer to Peer (P2P)	<p>(Your HMP must be licensed for P2P.) Enter the Haivision P2P key to enable the ability to configure locations for P2P HLS streaming. See Configuring HMP for Haivision Peer-to-Peer Video Delivery for more details.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9c4;"> <p>⚠ Important</p> <p>Haivision Peer-to-Peer on HMP is currently in Preview Mode.</p> </div>
--------------------	--


Installing System Updates

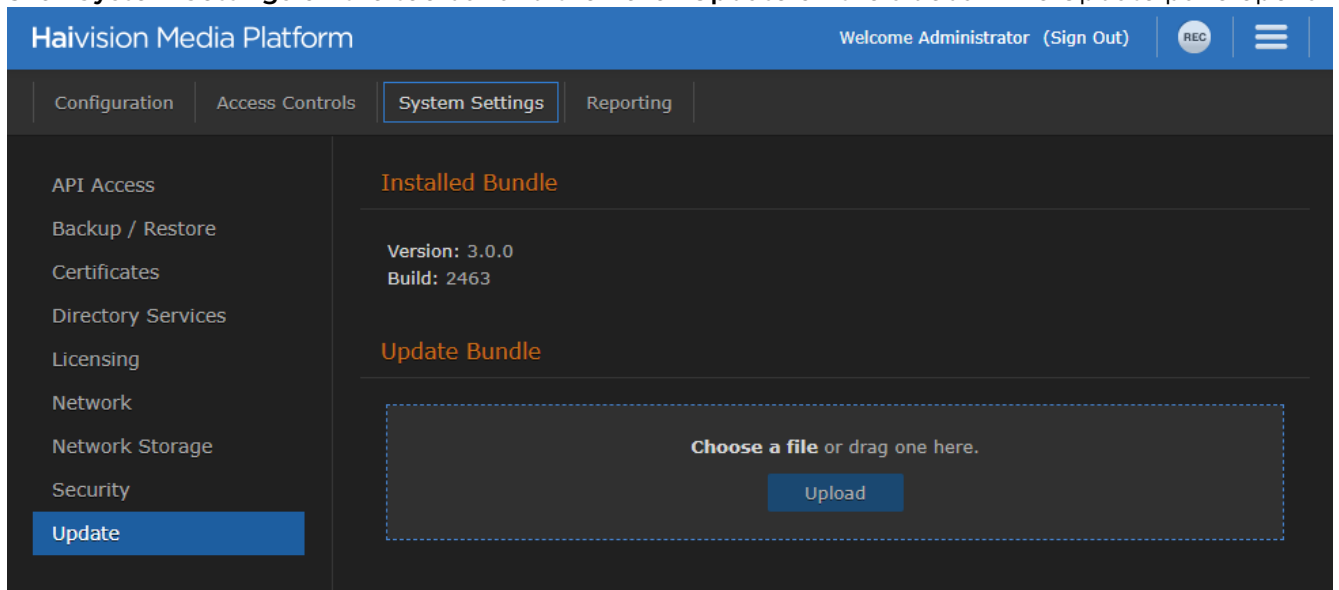
When you first receive the Haivision Media Platform appliance, the necessary software is pre-installed on it. System updates are available for download through the [Haivision Support Portal](#). When a system update becomes available, you can easily install it from the Web interface after downloading the file to your local computer or network.

⚠ Note

- For major releases or when adding new features, you must apply a valid license key before updating (see [Licensing Your HMP](#)). Please contact Haivision Technical Support to obtain a valid license key.
- Only customers under a maintenance agreement can obtain an update package. If you install an update without a valid license key, HMP will not function.
- You cannot install system updates from a mobile device.

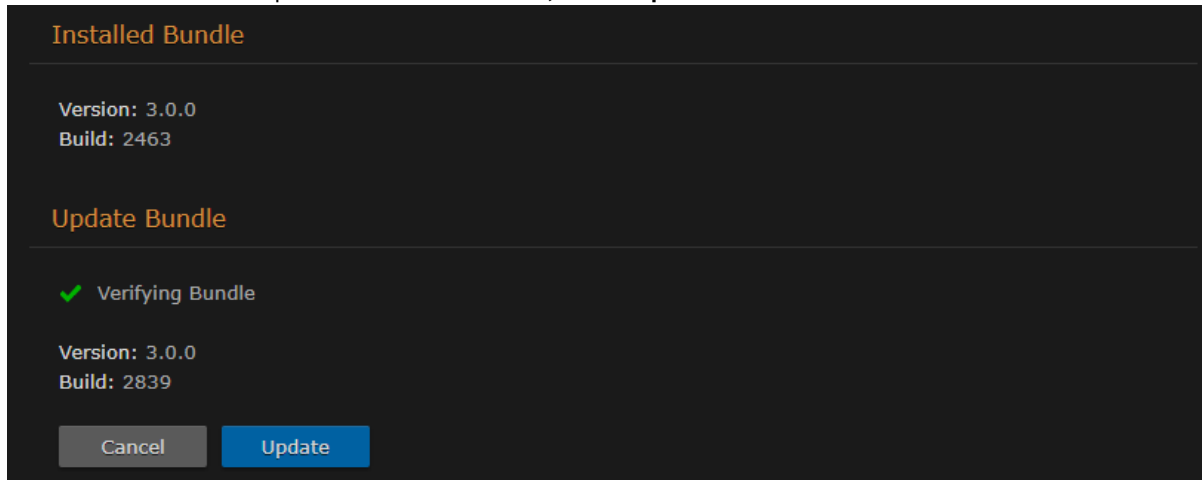
To install a system update:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **System Settings** on the toolbar and then click **Update** on the sidebar. The Update pane opens:



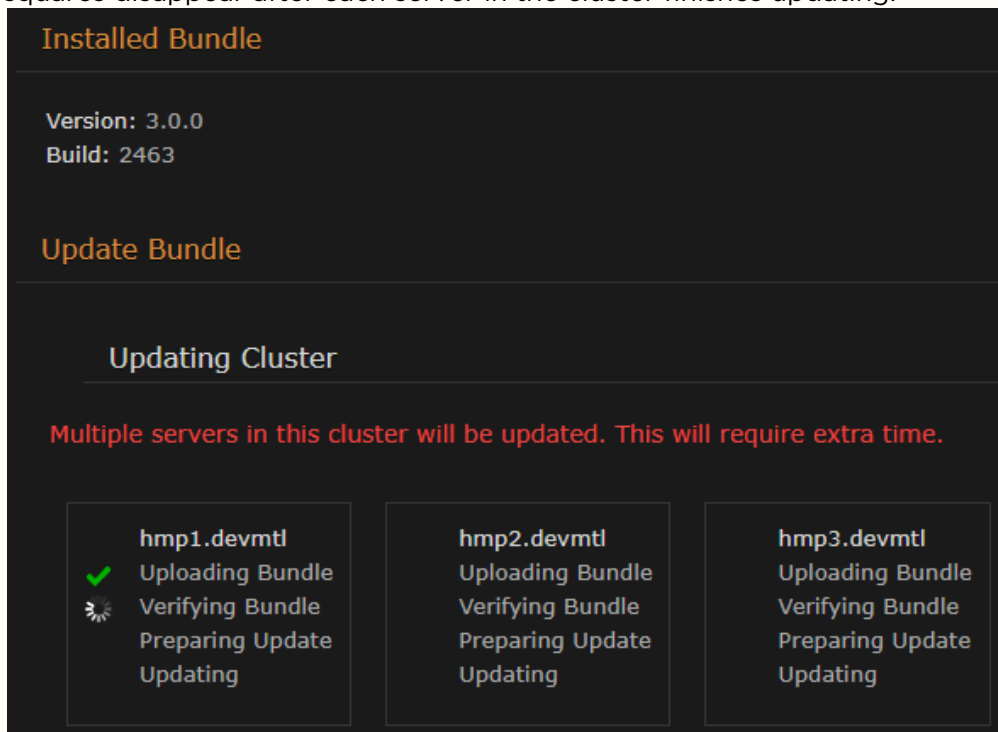
3. Drag an update bundle (titled `Haivision_Media_Platform-x.x.x_rxxxx_RELEASE.hai`) to the drop area or click **Choose a file** to select a bundle to load.
4. A confirmation appears showing the filename. Click **Upload** to continue. The progress bar shows the progress of the upload.

5. After the bundle is uploaded and verified, click **Update** and then click **Confirm**.



Note

For appliances that are part of an HA cluster, the update screen appears as below. The squares disappear after each server in the cluster finishes updating.



6. Wait until the update is complete and your HMP system reboots.
7. After the reboot and update completes, the browser displays a dialog indicating the update is complete. Click the **OK** button and the HMP Sign-in screen appears. If not, refresh your browser.
8. Sign in and ensure the system is functional.

Note

If updating from HMP version 2.6 to 3.0+ and your system uses Network Storage, after signing in you may notice that various assets (video sessions, sources, branding images, etc.) do not appear. To migrate your assets to the new version:

1. On the Administration screen, click **System Settings** on the toolbar and click **Network Storage** on the sidebar.
2. Under Network Storage Migration, click the **Migrate** button.
3. After a few minutes the migration process completes. Reboot the system and confirm that all data is restored and functional. Contact [Haivision Support](#) if assistance is necessary.

Reverting an Upgrade

If you have an upgrade that was not successful or if an existing installation has quit working properly, use the following procedure to revert (or rollback) to the previously installed version.

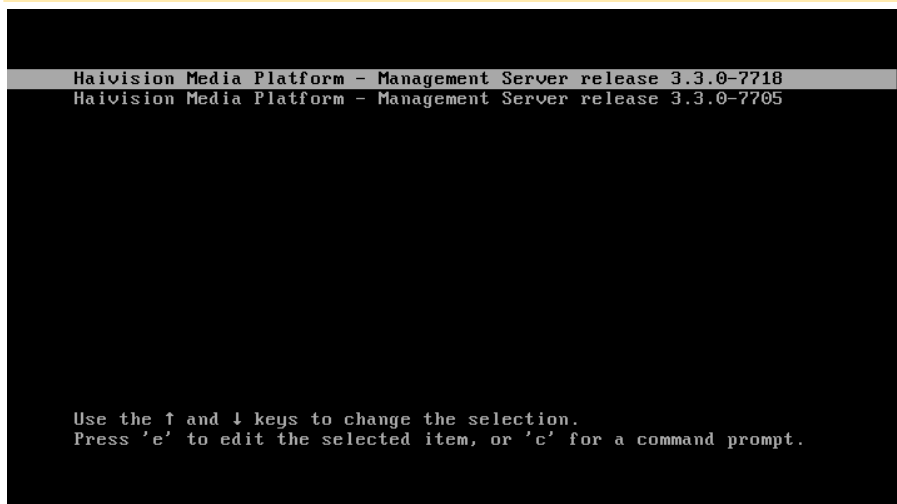
Note

If you have an HMP server, you must perform this procedure at its physical location.

1. If applicable, attach a monitor, keyboard, and mouse to the server. (See [Connecting the Server](#) for connection details.)
2. Reboot the device.
3. After the BIOS loads, when the following screen appears on the monitor immediately move the cursor to the previous version using the ↑ or ↓ arrow keys.

Note

You only have a few seconds to move the cursor before the bootloader starts the default version. If you take too long, return to step 2 and restart the system.



4. Ensure the previous version is selected, and press the **Enter** key.

After the system starts, you can try reinstalling the upgrade again or contact [Haivision Support](#) for assistance.

 **Tip**

- If you choose not to upgrade again, subsequent reboots will require you to perform this procedure to boot into the older version. Contact [Haivision Support](#) for instructions on changing the bootloader's default version.
- Videos, sessions, sources, and branding images are retained after reverting the upgrade.

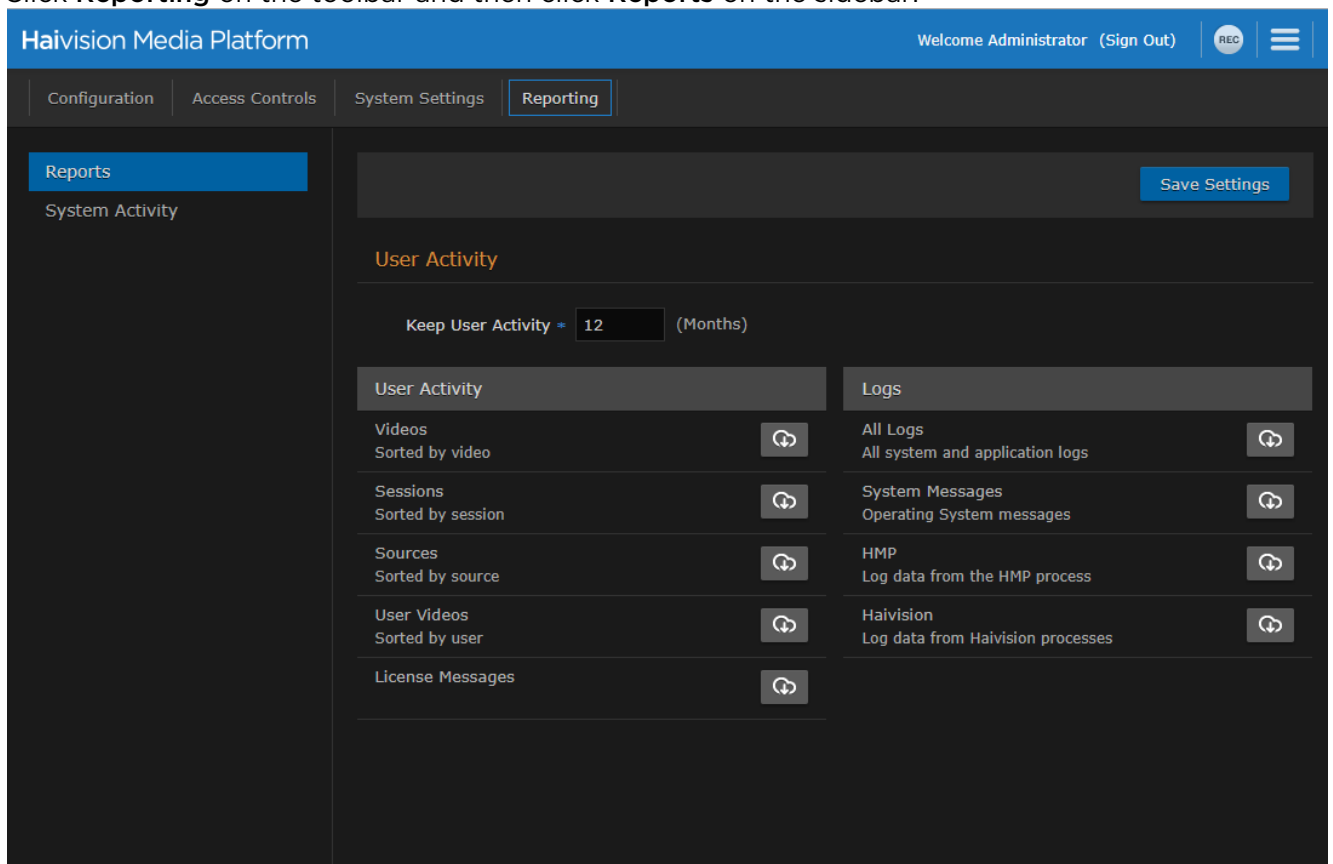
Reporting

The Administration Reporting screen includes two panes: Reports and System Activity.

The Reports pane lists user activity reports and system logs that you can download in .CSV file format. For the list of available reports and logs, see [Reports and Logs](#).

To view the reports:

1. Click the  icon on the banner and select **Administration** from the navigation drop-down menu.
2. Click **Reporting** on the toolbar and then click **Reports** on the sidebar.



3. To change how long to keep the user activity data, enter the number of months in the Keep User Activity field and click **Save Settings**.

 **Note**

User activity data older than the specified time period is automatically deleted by the system.

4. To download an activity report or log to your local system, click the  icon.

Topics Discussed

- [Reports and Logs](#)
- [Viewing System Activity](#)
- [Viewing High Availability Cluster Status](#)

Reports and Logs

The following tables list the available reports and logs.

[User Activity](#) [Logs](#) [P2P Analytics](#)

Each of the available user activity reports (in CSV file format) include the following:

- ID of the user performing the activity (for Web viewers) or the device ID (for STBs)
- UUID of the associated item
- Start time of the activity
- Name or title of the item
- The action taken (WATCH, DOWNLOAD, EDIT, SHARE, DELETE, etc.)
- A URL link to launch it
- stime (start time) in extended ISO format

⚠ Note

The time span of the list matches the time limit (number of months) specified in the Keep User Activity field, or covers activity from system startup through the current time, if less than the specified limit.

Report Item	Description
Videos	Activities sorted by video title. ⚠ Note The Videos report logs all recording viewing activity. It shows either the username for Web viewers or the device ID for STBs, the UUID, time, title, action, and launch URL.
Sessions	Activities sorted by session title.
Sources	Activities sorted by source title. ⚠ Note The Sources report logs all source viewing activity. It is intended to log user activity and STB activity.
User Videos	Activities sorted by user.

Report Item	Description
License Messages	<p>A list of occurrences when licensed bandwidth has been exceeded.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>⚠ Note After the initial occurrence, a new occurrence is reported only after the bandwidth has dropped and then when licensed bandwidth has been exceeded again.</p> </div> <p>The report includes data Type, Time, and Message, for example, “<code>Output bandwidth limit reached (bps): total usage:8629400(babel:8629400 hls:0), max allowed:8000000.</code>”</p>

User Activity [Logs](#) [P2P Analytics](#)

The available log files are:

Log Item	Description
All Logs	All system and application logs.
System Messages	A log of messages generated by the operating system.
Media Platform	Log data from HMP processes.
Haivision	Log data from Haivision processes.

User Activity [Logs](#) [P2P Analytics](#)

If licensed for your system, a button appears which links you to the Haivision P2P analytics dashboard. See [Configuring HMP for Haivision Peer-to-Peer Video Delivery](#) for details on using the Haivision P2P with HMP.

Viewing System Activity


The System Activity pane summarizes:

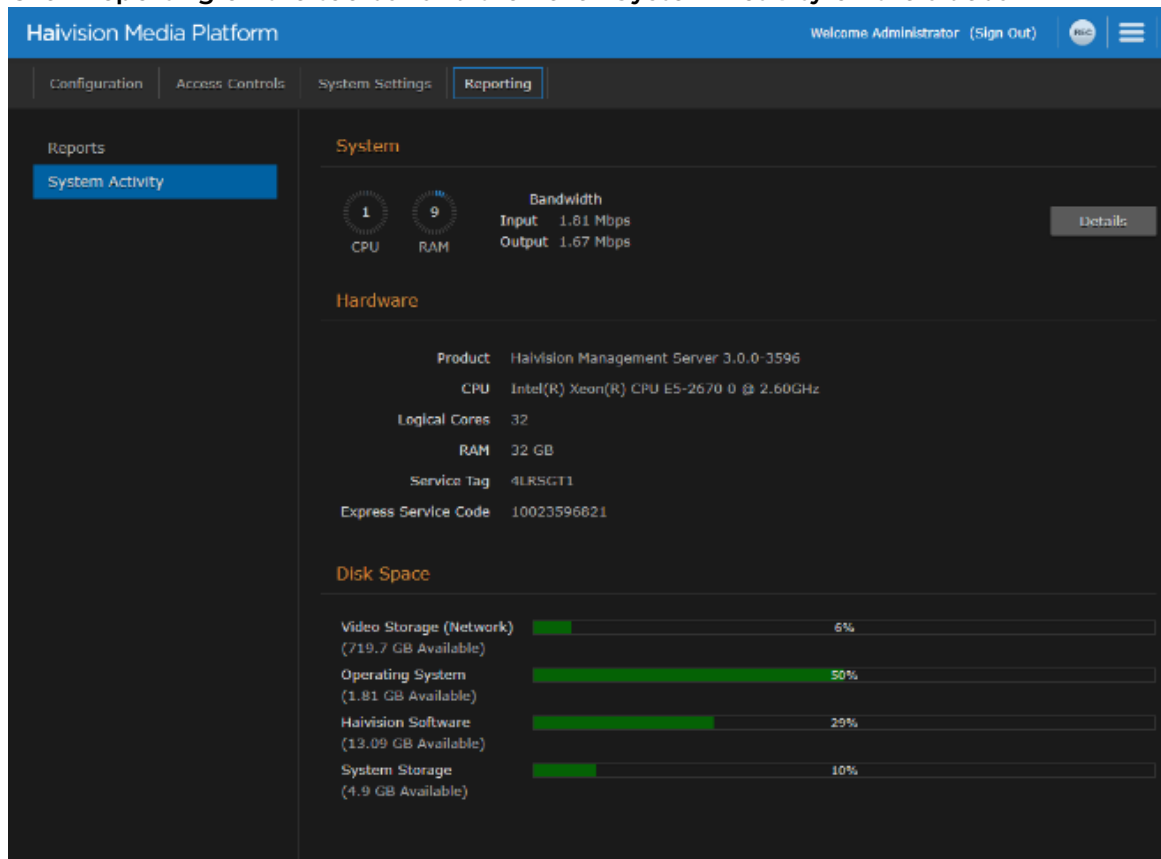
- Real-time system status information, such as CPU and memory usage, and I/O bandwidth bitrates, with the option to view graphical details.
- Hardware details, including whether HMP is running on a VM or a Haivision appliance.
- The available space for (local) video storage, operating system, Haivision software, and system storage (in GBs available, as well as percent used).

Note

Haivision recommends that you expand the VM disk when the video storage reaches 90% or more of the available space.

To view the System Activity:

1. Click the  icon and select **Administration** from the navigation drop-down menu.
2. Click **Reporting** on the toolbar and then click **System Activity** on the sidebar.



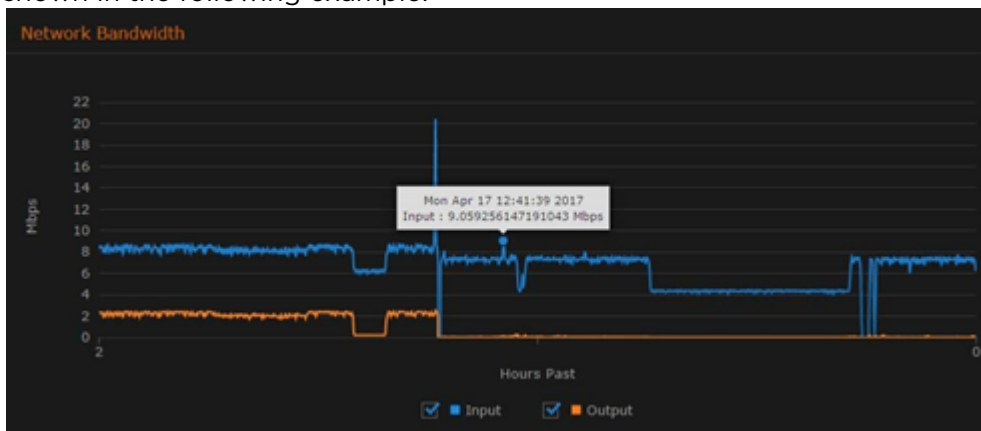
Tip

The color of the bars in the Disk Space graph change to orange when the space used on disk reaches 75%, and then to red when it reaches 90%.

- To view graphs of the network bandwidth, CPU, and memory click **Details**.
The X-axis units are days, hours, or minutes past (corresponding to the selected Time Scale). The Y-axis units are as follows:
 - Network bandwidth usage (in Megabits per second)
 - CPU load usage (in percent)
 - Memory usage (in percent)



- You can adjust the refresh rate (from 1 second to 30 minutes) and the time scale (from 5 minutes to 30 days past) for the graphs.
- To fine-tune the bandwidth usage graph, select the data to include: input and/or output (playback).
- To display an exact reading for the time and usage, you can mouse-over any of the graph lines, as shown in the following example:



Related Topics

- [Viewing High Availability Cluster Status](#)

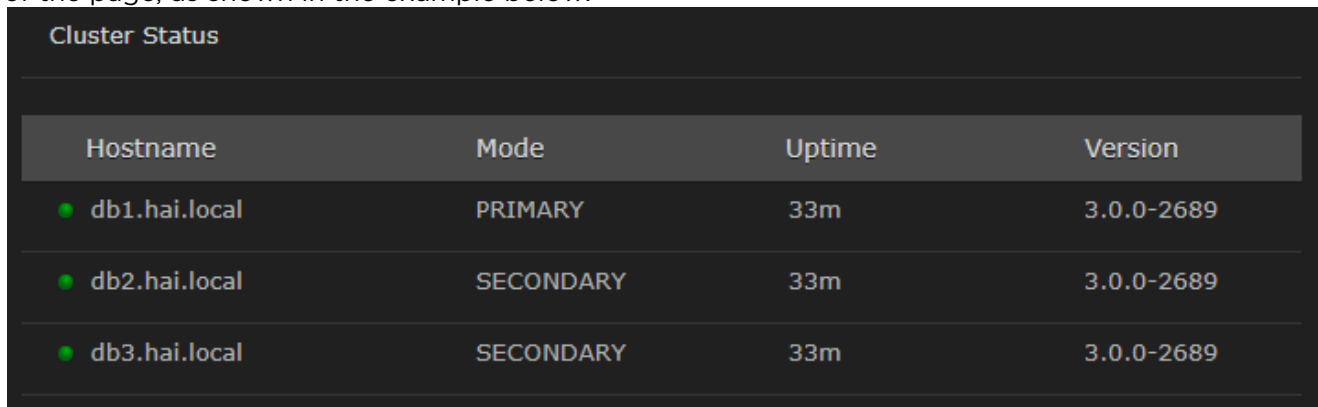
Viewing High Availability Cluster Status

If your system has High Availability (HA) clustering support, you can monitor cluster status at a glance from the System Activity page.

To view the HA cluster's status:

1. On the Administration screen, click **Reporting** on the toolbar and then click **System Activity** on the sidebar.

If the server is part of an HA cluster, the status of all servers in the cluster is shown on the bottom of the page, as shown in the example below.



Cluster Status			
Hostname	Mode	Uptime	Version
● db1.hai.local	PRIMARY	33m	3.0.0-2689
● db2.hai.local	SECONDARY	33m	3.0.0-2689
● db3.hai.local	SECONDARY	33m	3.0.0-2689

Related Topics

- [High Availability Clustering Failover Support](#)

KLV Dictionary Format

✓ Tip

These topics do not apply to the low-latency player, as a KLV dictionary is not needed for that player.

For the legacy Flash-based player, a KLV dictionary is necessary to display KLV data. This section lists the requirements for the dictionary format.

⚠ Note

A sample dictionary file is available from the [Haivision Support Portal](#).

Topics Discussed

- [Dictionary Syntax](#)
 - [Item - Translation](#)
 - [Item - Translation/Format/Suffix/Precision](#)
 - [Item - Enum](#)
- [64-bit Integer](#)

Dictionary Syntax

A dictionary must have a top-level attribute "items" whose type is a list. It contains a list of Local Data Sets (LDS) or items to be decoded. A LDS or item is matched by its universal key (e.g. the universal key of UAS is "06 0E 2B 34 02 0B 01 01 0E 01 03 01 01 00 00 00").

A LDS has also a list of items. Each item can be either of type "item" or "lds" (see example below).

```
{
  "items": [{
    "type": "lds",
    "name": "uas",
    "key": "06 0E 2B 34 02 0B 01 01 0E 01 03 01 01 00 00 00",
    "items": [
    ]
  }
  ]
}
```

Item - Translation

An item can be modified by a translation object. For example:

```
{
  "type": "item",
  "key": "25",
  "format": "uint16",
  "translation": {
    "multiplier": 0.30365453574425879301136797131304,
    "error": 2147483648,
    "addend": -900
  },
  "name": "Frame Center Elevation"
}
```

If the raw value of item 25 (a 16-bit unsigned integer) is equal to 2147483648, then the decoded value will be the string "error". Otherwise, the decoded value will be the raw value multiplied by 0.30365453574425879301136797131304 and subtracted by 900.

For example:

```
"25": {
  "value": 1000.88
}
```

You can also specify a key for the addend and that key's addend will be used. For example:

```
"addend": {
  "key": "23"
},
```

The default addend is 0.

Item - Translation/Format/Suffix/Precision

The displayValue attribute is formatted according to the format, suffix and precision attributes. If a format is supplied, the suffix and precision are ignored.

format

Supported formats: time, latitude, longitude.

suffix

The value of the suffix is appended to the value.

precision

The precision controls how many digits there are after the decimal point.

Examples

[Suffix/Precision](#) [Format](#)

```
{
  "type": "item",
  "key": "5",
  "format": "uint16",
  "translation": {
    "multiplier": 0.0054932478828107118333714808880751,
    "suffix": "°",
    "precision": 2
  },
  "name": "Platform Heading Angle"
}
```

```
{
  "value": 22.0664,
  "displayValue": "22.07°",
  "name": "Platform Heading Angle"
}
```

The second section shows what is sent to Haivision Media Platform based on the dictionary.

Suffix/Precision Format

```
{
  "type": "item",
  "key": "13",
  "format": "int32",
  "translation": {
    "multiplier": 4.19095158772121723169517574444512e-8,
    "addend": 0,
    "error": 2147483648,
    "format": "latitude"
  },
  "name": "Sensor Latitude"
}
```

```
{
  "value": -34.84,
  "displayValue": "034°50'24\" S",
  "name": "Sensor Latitude"
}
```

Common suffixes include " °C", "°", "m/s", and "m".

Item - Enum

An item can be modified by an enum object. The enum object can either have a "values" attribute or a "bits" attribute.

Values Attribute Bits Attribute

Example:

```
{
  "type": "item",
  "key": "34",
  "format": "uint8",
  "enum": {
    "values": {
      "0": "Detector off",
      "1": "No icing Detected",
      "2": "Icing Detected"
    }
  }
}
```

The values attribute is a mapping between the raw value (a 8-bit unsigned integer) and a string. If the raw value is 1, then the decoded value is the string "No icing Detected".

```
{
  name: "Icing detected"
  value: "No icing detected"
}
```

[Values Attribute](#) [Bits Attribute](#)

Example:

```
{
  "type": "item",
  "key": "47",
  "format": "uint8",
  "enum": {
    "bits": {
      "1": {
        "name": "Laser Range",
        "values": {
          "0": "off",
          "1": "on"
        }
      },
      "2": {
        "name": "Auto-Track",
        "values": {
          "0": "off",
          "1": "on"
        }
      },
      "3": {
        "name": "IR Polarity",
        "values": {
          "0": "blk",
          "1": "wht"
        }
      },
      "4": {
        "name": "Icing detected",
        "values": {
          "0": "off/no ice",
          "1": "on"
        }
      },
      "5": {
        "name": "Slant Range",
        "values": {
          "0": "calc",
          "1": "measured"
        }
      },
      "6": {
        "name": "Image Invalid",
        "values": {
          "0": "valid",
          "1": "invalid"
        }
      }
    }
  }
}
```

The bits object is a mapping between each bit of the raw value and a string. If the raw value of item 47 (a 8-bit unsigned integer) is 3 (0000 0011). Then, the decoded value is:


```
"47": {
  "value": {
    "1": {
      "value": "on",
      "name": "Laser Range"
    },
    "2": {
      "value": "on",
      "name": "Auto-Track"
    },
    "3": {
      "value": "blk",
      "name": "IR Polarity"
    },
    "4": {
      "value": "off/no ice",
      "name": "Icing detected"
    },
    "5": {
      "value": "calc",
      "name": "Slant Range"
    },
    "6": {
      "value": "valid",
      "name": "Image Invalid"
    },
    "7": null,
    "8": null
  }
}
```

Since we did not specify a mapping for bits 7 and 8, they are set to null.

64-bit Integer

64-bit integers are converted to a string because JavaScript does not support 64-bit integers.

Technical Specifications

This section lists the technical specifications for Haivision Media Platform (HMP).

Topics Discussed

- [Haivision Media Platform Software](#)
- [Haivision Media Platform Hardware](#)

Haivision Media Platform Software

	Workgroup Edition	Enterprise Edition
Standard Features	5 recording ports 200 sources 500 concurrent users Web-based admin & management Multi-stream viewing & recording Video-on-demand library Network file storage User generated content/watch-folder ingest User authentication with LDAP/AD/SSO Roles-based and permissions HTML5 or Flash Player Set-top box management Content, system, and user activity reporting Expandable license options	
Edition-based Features	Live Review - monitor content during record	IPTV channel lineups 608/708 Closed Captions User-selectable alt-language tracks Haivision Media Gateway (with encryption)
Expandable Features	2,500 user/device license packs 5 recording channel packs IPTV and channel guide VOD portal/content library eCDN (requires Haivision Media Gateway) High Availability (requires use of network storage)	2,500 user/device license packs 5 recording channel packs eCDN (requires Haivision Media Gateway) High Availability (requires use of network storage) Haivision Peer-to-Peer HLS streaming
Management Interfaces	HMP Portal REST API Command Line API Console UI	
Audio/Video Formats	H.264 AAC-ADTS Audio	

	Workgroup Edition	Enterprise Edition
Inputs	MPEG-2 Transport Stream SRT (Secure Reliable Transport) RTSP/RTMP (requires HMG)	
Output	MPEG-2 Transport Stream SRT (Secure Reliable Transport) HLS (with end-to-end encryption) RTMP, RTMPS	

Haivision Media Platform Hardware

The HMP server appliance is based on the Dell PowerEdge R640 rack server:

	Workgroup Edition	Enterprise Edition
Dimensions (mm)	1RU: 42.8H x 482.38W x 794.77D	
Operating System	Secure Linux-based OS	
Processor	Dual Intel® Xeon® processors	
Power Supplies	Redundant hot-swappable power supplies, 100-240 VAC	
Storage	RAID-5 configuration w/ hot-swappable drives (1.8TB)	RAID-5 configuration w/ 2.1TB (effective)
Maximum Weight	21.9 kg	
Network	2x GigE Base-T 2x SFP+ (up to 10Gbps) expansion slots (modules not included)	
Performance	Rated up to 1,500Mbps (300 streams @ 5Mbps)	

Warranties

1-Year Limited Hardware Warranty

Haivision warrants its hardware products against defects in materials and workmanship under normal use for a period of ONE (1) YEAR from the date of equipment shipment ("Warranty Period"). If a hardware defect arises and a valid claim is received within the Warranty Period, at its option and to the extent permitted by law, Haivision will either (1) repair the hardware defect at no charge, or (2) exchange the product with a product that is new or equivalent to new in performance and reliability and is at least functionally equivalent to the original product. A replacement product or part assumes the remaining warranty of the original product or ninety (90) days from the date of replacement or repair, whichever is longer. When a product or part is exchanged, any replacement item becomes your property and the replaced item becomes Haivision's property.

EXCLUSIONS AND LIMITATIONS

This Limited Warranty applies only to hardware products manufactured by or for Haivision that can be identified by the "Haivision" trademark, trade name, or logo affixed to them. The Limited Warranty does not apply to any non-Haivision hardware products or any software, even if packaged or sold with Haivision hardware. Manufacturers, suppliers, or publishers, other than Haivision, may provide their own warranties to the end user purchaser, but Haivision, in so far as permitted by law, provides their products "as is".

Haivision does not warrant that the operation of the product will be uninterrupted or error-free. Haivision does not guarantee that any error or other non-conformance can or will be corrected or that the product will operate in all environments and with all systems and equipment. Haivision is not responsible for damage arising from failure to follow instructions relating to the product's use.

This warranty does not apply:

- (a) to cosmetic damage, including but not limited to scratches, dents and broken plastic on ports;
- (b) to damage caused by accident, abuse, misuse, flood, fire, earthquake or other external causes;
- (c) to damage caused by operating the product outside the permitted or intended uses described by Haivision;
- (d) to a product or part that has been modified to alter functionality or capability without the written permission of Haivision; or
- (e) if any Haivision serial number has been removed or defaced.

TO THE EXTENT PERMITTED BY LAW, THIS WARRANTY AND REMEDIES PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, REMEDIES AND CONDITIONS, WHETHER ORAL OR WRITTEN, STATUTORY, EXPRESS OR IMPLIED. AS PERMITTED BY APPLICABLE LAW, HAIVISION SPECIFICALLY DISCLAIMS ANY AND ALL STATUTORY OR IMPLIED WARRANTIES,

INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND WARRANTIES AGAINST HIDDEN OR LATENT DEFECTS. IF HAIVISION CANNOT LAWFULLY DISCLAIM STATUTORY OR IMPLIED WARRANTIES THEN TO THE EXTENT PERMITTED BY LAW, ALL SUCH WARRANTIES SHALL BE LIMITED IN DURATION TO THE DURATION OF THIS EXPRESS WARRANTY AND TO REPAIR OR REPLACEMENT SERVICE AS DETERMINED BY HAIVISION IN ITS SOLE DISCRETION. No Haivision reseller, agent, or employee is authorized to make any modification, extension, or addition to this warranty. If any term is held to be illegal or unenforceable, the legality or enforceability of the remaining terms shall not be affected or impaired.

EXCEPT AS PROVIDED IN THIS WARRANTY AND TO THE EXTENT PERMITTED BY LAW, HAIVISION IS NOT RESPONSIBLE FOR DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR CONDITION, OR UNDER ANY OTHER LEGAL THEORY, INCLUDING BUT NOT LIMITED TO LOSS OF USE; LOSS OF REVENUE; LOSS OF ACTUAL OR ANTICIPATED PROFITS (INCLUDING LOSS OF PROFITS ON CONTRACTS); LOSS OF THE USE OF MONEY; LOSS OF ANTICIPATED SAVINGS; LOSS OF BUSINESS; LOSS OF OPPORTUNITY; LOSS OF GOODWILL; LOSS OF REPUTATION; LOSS OF, DAMAGE TO OR CORRUPTION OF DATA; OR ANY INDIRECT OR CONSEQUENTIAL LOSS OR DAMAGE HOWSOEVER CAUSED INCLUDING THE REPLACEMENT OF EQUIPMENT AND PROPERTY, ANY COSTS OF RECOVERING, PROGRAMMING, OR REPRODUCING ANY PROGRAM OR DATA STORED OR USED WITH HAIVISION PRODUCTS AND ANY FAILURE TO MAINTAIN THE CONFIDENTIALITY OF DATA STORED ON THE PRODUCT. THE FOREGOING LIMITATION SHALL NOT APPLY TO DEATH OR PERSONAL INJURY CLAIMS, OR ANY STATUTORY LIABILITY FOR INTENTIONAL AND GROSS NEGLIGENT ACTS AND/OR OMISSIONS.

OBTAINING WARRANTY SERVICE

Before requesting warranty service, please refer to the documentation accompanying this hardware product and the Haivision Support Portal <https://support.haivision.com>. If the product is still not functioning properly after making use of these resources, please contact Haivision or Authorized Reseller using the information provided in the documentation. When calling, Haivision or Authorized Reseller will help determine whether your product requires service and, if it does, will inform you how Haivision will provide it. You must assist in diagnosing issues with your product and follow Haivision's warranty processes.

Haivision may provide warranty service by providing a return material authorization ("RMA") to allow you to return the product in accordance with instructions provided by Haivision or Authorized Reseller. You are fully responsible for delivering the product to Haivision as instructed, and Haivision is responsible for returning the product if it is found to be defective. Your product or a replacement product will be returned to you configured as your product was when originally purchased, subject to applicable updates. Returned products which are found by Haivision to be not defective, out-of-warranty or otherwise ineligible for warranty service will be shipped back to you at your expense. All replaced products and parts, whether under warranty or not, become the property of Haivision. Haivision may require a completed pre-authorized form as security for the retail price of the replacement product. If you fail to return the replaced product as instructed, Haivision will invoice for the pre-authorized amount.

APPLICABLE LAW

This Limited Warranty is governed by and construed under the laws of the Province of Quebec, Canada.

This Limited Hardware Warranty may be subject to Haivision's change at any time without prior notice.

EULA - End User License Agreement

READ BEFORE USING

THE LICENSED SOFTWARE IS PROTECTED BY COPYRIGHT LAWS AND TREATIES. READ THE TERMS OF THE FOLLOWING END USER (SOFTWARE) LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE ACCESSING THE LICENSED SOFTWARE. BY SCANNING THE QR CODE TO REVIEW THIS AGREEMENT AND/OR ACCESSING THE LICENSED SOFTWARE, YOU CONFIRM YOUR ACCEPTANCE OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, HAIVISION IS UNWILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AND YOU ARE NOT AUTHORIZED TO ACCESS THE LICENSED SOFTWARE.

Click the following link to view the Software End-User License Agreement: [Haivision EULA.pdf](#)

If you have questions, please contact legal@haivision.com

SLA - Service Level Agreement

1. Introduction

This Service Level and Support supplement forms a part of and is incorporated into the Service Agreement (the "Agreement") between You and Haivision Network Video Inc. ("Haivision"). Capitalized terms used but not otherwise defined in this supplement shall have the meaning ascribed to them in the Agreement. Haivision may, upon prior written notice to You, amend this supplement to incorporate improvements to the service levels and support commitments at no additional cost to You. This supplement applies only to those products and services set forth below.

2. Definitions

- "Audience Member" means an individual or entity that accesses Your Published Media Objects through a public URL.
- "Access Service" means the service provided by Haivision VCMS that verifies an Audience Member's credentials.
- "Digital Media File" means a computer file containing text, audio, video, or other content.
- "Outage" is a 12-minute period of consecutive failed attempts by all six agents to PING the domain on the Haivision Streaming Media network.
- "Published Media Object" means a Digital Media File with a public URL.
- "Transaction" means the creation of a right for an Audience Member to access a Media Object and the completion of an order logged in the order history service.

3. Service Levels for the Video Content Management System

The service levels in this [Section 3](#) apply only to the hosted version of Haivision VCMS and the Haivision VCMS development kit (collectively, the "Standard Hosted Components" of Haivision Video Cloud Services). Subject to the exceptions noted in [Section 4](#) below, the aforementioned components of Haivision Video Cloud Services will be available for use over the course of each calendar month as follows:

Type of Access	Definition	Availability Level
Write Functions	<ul style="list-style-type: none"> • Access to all functions through the administrative user interface. • Ability to add or modify objects and metadata through the application programming interface (“API”) • Ability of ingest service to check for new or updated files or feeds 	99.999%
Read-Only Functions	<ul style="list-style-type: none"> • Ability to retrieve data through the API • Ability for Audience Members to authenticate through the Access Service • Ability for Audience Members to play Published Media Objects • Ability for Audience Members to play Haivision VCMS-authenticated or entitled Published Media Objects • Ability to complete Transactions 	99.999%

4. Exceptions to Availability for the VCMS

The Standard Hosted Components may not be available for use under the following circumstances, and in such case such periods of unavailability shall not be counted against Haivision Video Cloud for purposes of calculating availability:

- a. Normal Maintenance, Urgent Maintenance and Upgrades as defined in the table below;
- b. Breach of the Agreement by You as defined in the Agreement;
- c. The failure, malfunction, or modification of equipment, applications, or systems not controlled by Haivision Video Cloud;
- d. Any third party, public network, or systems unavailability;
- e. Acts of Force Majeure as defined in the Agreement;
- f. Modification of software made available to You as part of Haivision Video Cloud Services by You or a third party acting on Your behalf; and
- g. Any third party product or service not incorporated into Haivision Video Cloud Services or any third party plug-in.

Haivision Video Cloud shall make commercially reasonable efforts to notify, or work with, applicable third parties to repair or restore Haivision VCMS functionality affected by such exceptions.

Type of Maintenance	Purpose	Write Functions Available	Read Functions Available	Maximum Time Per Month	Continuous Time in Mode (Max)	Window (Central Time)	Min Notice
Normal	<ul style="list-style-type: none"> • Preventive maintenance on the software/hardware components of Haivision VCMS • Addition of new features/functions • Repair errors that are not immediately affecting Your use of Haivision VCMS 	No	Yes	10 Hours	6 Hours	10:00p m - 5:00a m	48 Hours
Urgent	<ul style="list-style-type: none"> • Repair errors that are immediately affecting Your use of Haivision VCMS 	No	Yes	30 Minutes	15 Minutes	Any Time	3 Hours

Type of Maintenance	Purpose	Write Functions Available	Read Functions Available	Maximum Time Per Month	Continuous Time in Mode (Max)	Window (Central Time)	Min Notice
Upgrades	<ul style="list-style-type: none"> Perform upgrades on software or hardware elements necessary to the long term health or performance of Haivision VCMS, but which, due to their nature, require that certain components of Haivision VCMS to be shut down such that no access is possible 	No	No	1 Hour	1 Hour	12:00am - 4:00am M-F	5 Days

5. Credits for Downtime for the VCMS

Haivision Video Cloud will grant a credit allowance to You if You experience Downtime in any calendar month and you notify Haivision Video Cloud thereof within ten (10) business days after the end of such calendar month. In the case of any discrepancy between the Downtime as experienced by You and the Downtime as measured by Haivision Video Cloud, the Downtime as measured by Haivision Video Cloud shall be used to calculate any credit allowance set forth in this section. Such credit allowance shall be equal to the pro-rated charges of one-half day of Fees for each hour of Downtime or fraction thereof. The term “Downtime” shall mean the number of minutes that Standard Hosted Components are unavailable to You during a given calendar month below the availability levels thresholds in [Section 3](#), but shall not include any unavailability resulting from any of the exceptions noted in [Section 4](#). Within thirty (30) days after the end of any calendar month in which Downtime occurred below the availability levels thresholds in [Section 3](#), Haivision Video Cloud shall provide You with a written report detailing all instances of Downtime during the previous month. Any credit allowances accrued by You may be offset against any and all Fees owed to Haivision Video Cloud pursuant to the Agreement, provided that a maximum of one month of credit may be accrued per month.

6. Support Services for the VCMS

Support for Haivision Video Cloud Services as well as the Application Software (defined as the VCMS application software components that Haivision licenses for use in conjunction with the Video Cloud Services) can be reached at hvc-techsupport@haivision.com and shall be available for all Your support requests. Haivision Video Cloud will provide 24x7 monitoring of the Standard Hosted Components.

Cases will be opened upon receipt of request or identification of issue, and incidents will be routed and addressed according to the following:

Severity Level	Error State Description	Status Response Within	Incident Resolution within
1 - Critical Priority	Renders Haivision VCMS inoperative or causes Haivision VCMS to fail catastrophically.	15 minutes	4 hours
2 - High Priority	Affects the operation of Haivision VCMS and materially degrades Your use of Haivision VCMS.	30 minutes	6 hours
3 - Medium Priority	Affects the operation of Haivision VCMS, but does not materially degrade Your use of Haivision VCMS.	2 hours	12 hours

Severity Level	Error State Description	Status Response Within	Incident Resolution within
4 - Low Priority	Causes only a minor impact on the operation of Haivision VCMS.	1 business day	3 business days

7. Service Levels for Haivision Streaming Media Service

Haivision agrees to provide a level of service demonstrating 99.9% Uptime. The Haivision Streaming Media Service will have no network Outages.

The following methodology will be employed to measure Streaming Media Service availability:

Agents and Polling Frequency

- a. From six (6) geographically and network-diverse locations in major metropolitan areas, Haivision’s Streaming Media will simultaneously poll the domain identified on the Haivision Streaming Media network.
- b. The polling mechanism will perform a PING operation, sending a packet of data and waiting for a reply. Success of the PING operation is defined as a reply being received.
- c. Polling will occur at approximately 6-minute intervals.
- d. Based on the PING operation described in (b) above, the response will be assessed for the purpose of measuring Outages.

If an Outage is identified by this method, the customer will receive (as its sole remedy) a credit equivalent to the fees for the day in which the failure occurred.

Haivision reserves the right to limit Your use of the Haivision Streaming Media network in excess of Your committed usage in the event that Force Majeure events, defined in the Agreement, such as war, natural disaster or terrorist attack, result in extraordinary levels of traffic on the Haivision Streaming Media network.

8. Credits for Outages of Haivision Streaming Media Service

If the Haivision Streaming Media network fails to meet the above service level, You will receive (as your sole remedy) a credit equal to Your or such domain’s committed monthly service fee for the day in which the failure occurs, not to exceed 30 days of fees.

9. No Secondary End User Support

UNDER NO CIRCUMSTANCES MAY YOU PROVIDE CONTACT INFORMATION FOR HAIVISION SERVICES TO CUSTOMERS OR AUDIENCE MEMBERS OR OTHER THIRD PARTIES WITHOUT HAIVISION’S EXPRESS PRIOR WRITTEN CONSENT.

Getting Help

<p>General Support</p>	<p>North America (Toll-Free) 1 (877) 224-5445</p> <p>International 1 (514) 334-5445</p> <p><i>and choose from the following:</i> Sales - 1, Cloud Services - 3, Support - 4</p>
<p>Managed Services</p>	<p>U.S. and International 1 (512) 220-3463</p>
<p>Fax</p>	<p>1 (514) 334-0088</p>
<p>Support Portal</p>	<p>https://support.haivision.com</p>
<p>Product Information</p>	<p>info@haivision.com</p>

