HAIVISION

# Haivision Media Platform 3.0

## Administrator's Guide

HVS-ID-AG-HMP-30, Issue 01

# Edition Notice

## 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

## Reporting 169

## KLV Dictionary Format 175

## Technical Specifications 180

## Warranties 182

## Getting Help 188

# About This Document

## Conventions

The following conventions are used to help clarify the content.

### Typographic Conventions and Elements

| | |
|---|---|
| *Italics* | 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**.

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**.

# Introduction

**Important**

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

**Topics Discussed**

## New Product Features

The Haivision Media Platform (HMP) 3.0.1 maintenance release adds the following new features:

- Support for Haivision Play 4000 STBs
- Administrators can control the default SRT output latency on a per location basis
- The Manage Devices page displays the STB model when hovering over the device name

HMP 3.0 introduces the following new features and enhancements to existing capabilities:

- High Availability Clustering failover support
- Support for Haivision Play 2000 STBs
- User and Usage Content Analytics
- Architectural transition from CentOS 6 to CentOS 7 for continued supportability, compatibility, and advancement in the platform design
- Web UI enhancements, including updates and testing as WCAG 2.0 AA (Accessibility) Compliance
- Keyboard Shortcuts via Hotkeys

**Note**

These features vary by product edition and license.

**Related Topics**

- High Availability Clustering Failover Support
- Reporting and Analytics

## Haivision Media Platform Overview

Haivision Media Platform (HMP, formerly "Calypso") is a media recording, management and distribution platform designed to capture and share video content in real-time while providing organization and discoverability to video assets. HMP helps you organize, manage and share secure, high quality live and on-demand video to viewers on any screen/device – desktops, monitors and mobile devices – anywhere.

Haivision Media Platform offers three product editions to allow you to choose the best solution for your organization:

- Enterprise Edition → All Hands,
- Site Edition → IPTV
- Workgroup Edition → Performance Recording

For more information, see **Product Editions**.

Haivision Media Platform is available as an on-premise solution (server appliances and/or VM appliances), cloud (on private data centers as well as leading public clouds), and as a hybrid solution (hosted in cloud or on-premises or both), with video distribution options tailored to each unique need and network infrastructure.

For information on server appliances, see **Physical Description (Servers)**.

**Topics Discussed**

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

## Product Features

Key Haivision Media Platform features include the following:

### Stream, Record, Play

Live stream, record multiple HD sources, or watch IPTV or VOD content.

- Broadcast live all hands and town hall meetings so employees can watch from remote offices, off-site locations or on the road.
- Live stream and record multiple HD sources simultaneously for multi-view, real-time monitoring.
- Deliver broadcast TV channels along with live internal content throughout your organization.
- Share videos and pre-recorded content (Video-On-Demand) with authenticated viewers.

### Permission-Based Authentication

Support for Active Directory, LDAP and SSO ensures that administrators can easily and securely provision employees and set-top boxes with access to the designated content.

### Security

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

### Multicast/Unicast

Standards-based support for unicast and multicast ensures minimal IT intervention for WAN/LAN infrastructure.

### Multisite eCDN (Enterprise Content Delivery Network)

Distribute live video to multiple locations worldwide without overwhelming the network.

### High Quality Players

Haivision's hardware and software players provide broadcast-quality viewing experiences on any device.

### Set-Top Box Management

Centrally manage and schedule when and where your video is displayed – in hallways, public areas, conference rooms, and auditoriums.

### Metadata Tagging

Apply file-based and real-time metadata tags and keywords to make important content easy to find and manage.

### Hybrid/Cloud

On-premise, cloud and hybrid video distribution options fit your unique needs and network infrastructure.

### SRT

Haivision's SRT (Secure Reliable Transport) technology enables the delivery of encrypted, high performance video over the public Internet.

### Watch On Any Screen

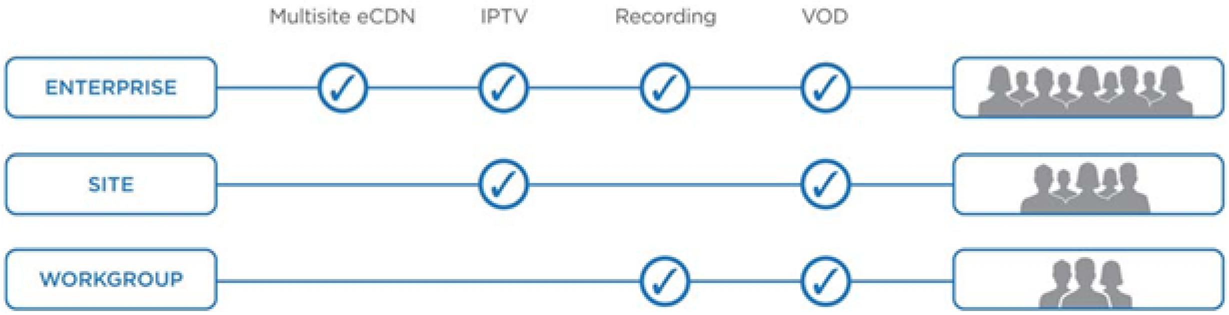
Deliver video securely to any screen, including desktops, mobile devices, and televisions.
See Haivision Play for more information.

### Enterprise Integration

Easily publish live and on-demand video to third-party portals such as Microsoft Share Point.

## Product Editions

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

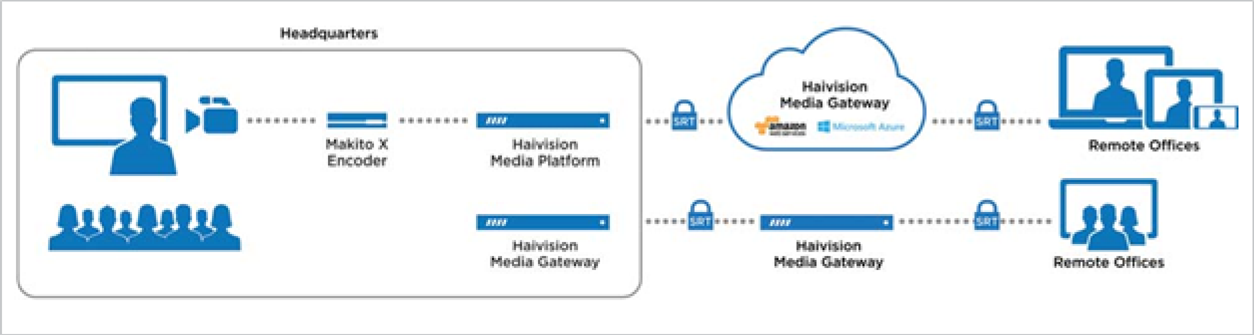


| | Multisite eCDN | IPTV | Recording | VOD |
|---|---|---|---|---|
| ENTERPRISE | ✓ | ✓ | ✓ | ✓ |
| SITE | | ✓ | | ✓ |
| WORKGROUP | | | ✓ | ✓ |

## Enterprise Edition

**Broadcast and Record All Hands, Town Halls and Internal Live Events Across Multiple Locations**

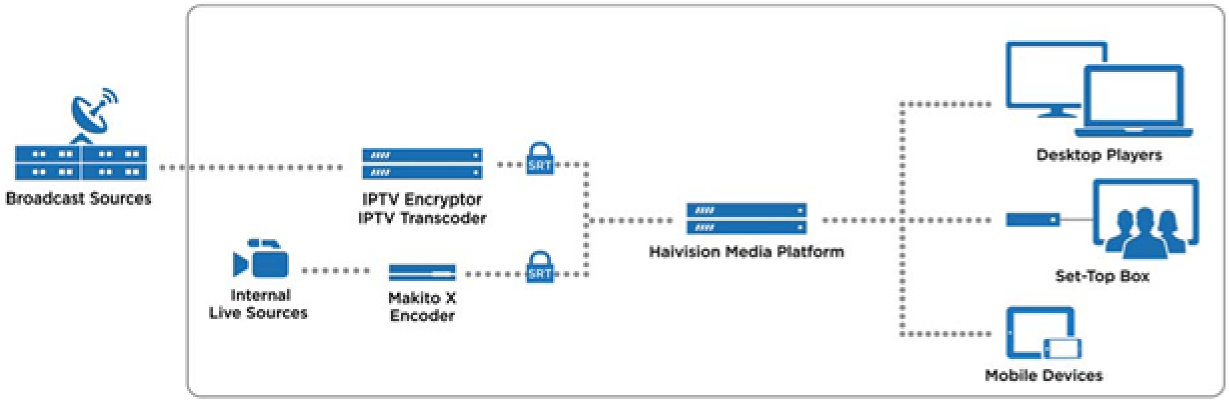
The Haivision Media Platform **Enterprise Edition** enables you to securely distribute live and on-demand broadcast-quality video, such as CEO all-hands, company events, HR updates, product launches and IPTV to employees watching on any screen at headquarters, remote offices, and on the road.



## Site Edition

**Distribute IPTV and Live Corporate Content to All Screens, Desktops and Devices in a Single Location**

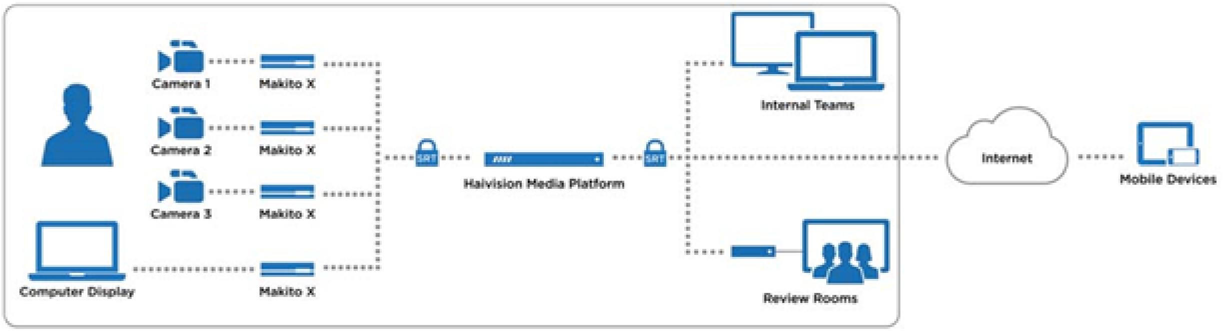
The Haivision Media Platform **Site Edition** enables you to manage and deliver broadcast television channels and other live content throughout your facility, including auditoriums, lobbies, break rooms, and conference areas. The Site Edition is available in Base, Advanced, and Advanced VOD versions, from 10 live channels/100 concurrent users maximum, to up to 500 live channels/500 concurrent users.



## Workgroup Edition

**Performance Recording for Research Teams and Training Facilities**

The Haivision Media Platform **Workgroup Edition** is designed to enable teams to watch and record multiple synchronized HD video sources for review and analysis. Users can apply metadata to track and manage important moments in the video. This edition is ideal for research, including usability testing, focus groups, simulations, and training. The **Workgroup Edition** is available in 5-1, 25-1, and 50-1 versions, supporting from 5 to 25 to 50 concurrent recording streams.



**Note**

Licensed features per Edition include the maximum number of sources/IPTV channels, maximum number of concurrent recordings, and Video On Demand (VOD).
Haivision Media Platform Editions are expandable through licensing. For detailed information, please refer to Haivision's website at: https://www.haivision.com

## 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.

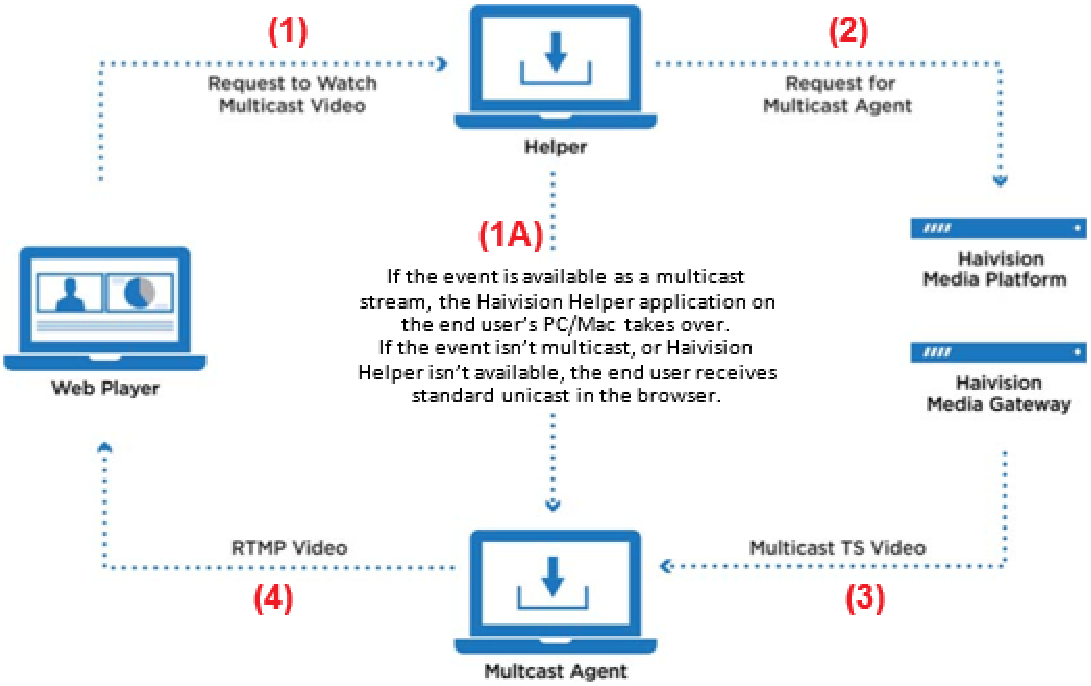
Following is a description of the process by which the Helper launches the multicast agent and enables multicast support:

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.


(1)
Request to Watch Multicast Video
Helper
(2)
Request for Multicast Agent
(1A)
If the event is available as a multicast stream, the Haivision Helper application on the end user's PC/Mac takes over. If the event isn't multicast, or Haivision Helper isn't available, the end user receives standard unicast in the browser.
Web Player
Haivision Media Platform
Haivision Media Gateway
RTMP Video
(4)
Multicast TS Video
(3)
Multcast Agent

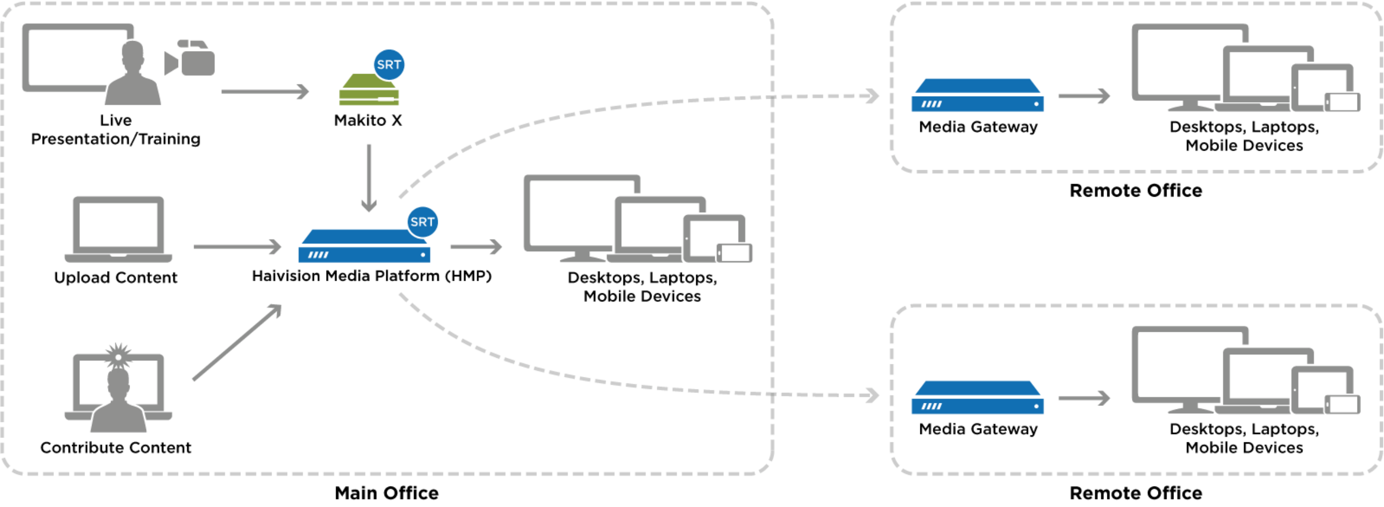
4. **Multicast TS Video:** The multicast agent joins the Multicast Group, and negotiates access and encryption for the video.
5. **RTMP Video:** The multicast agent converts the stream from Multicast TS to Native Web Video (RTMP is used for low latency), and the RTMP stream is delivered securely to the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

**Note**

For the latest information, please refer to the Haivision Helper Installation Guide.

## 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.



### Related Topics

- Configuring HMP-Media Gateway Pairings

## 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**

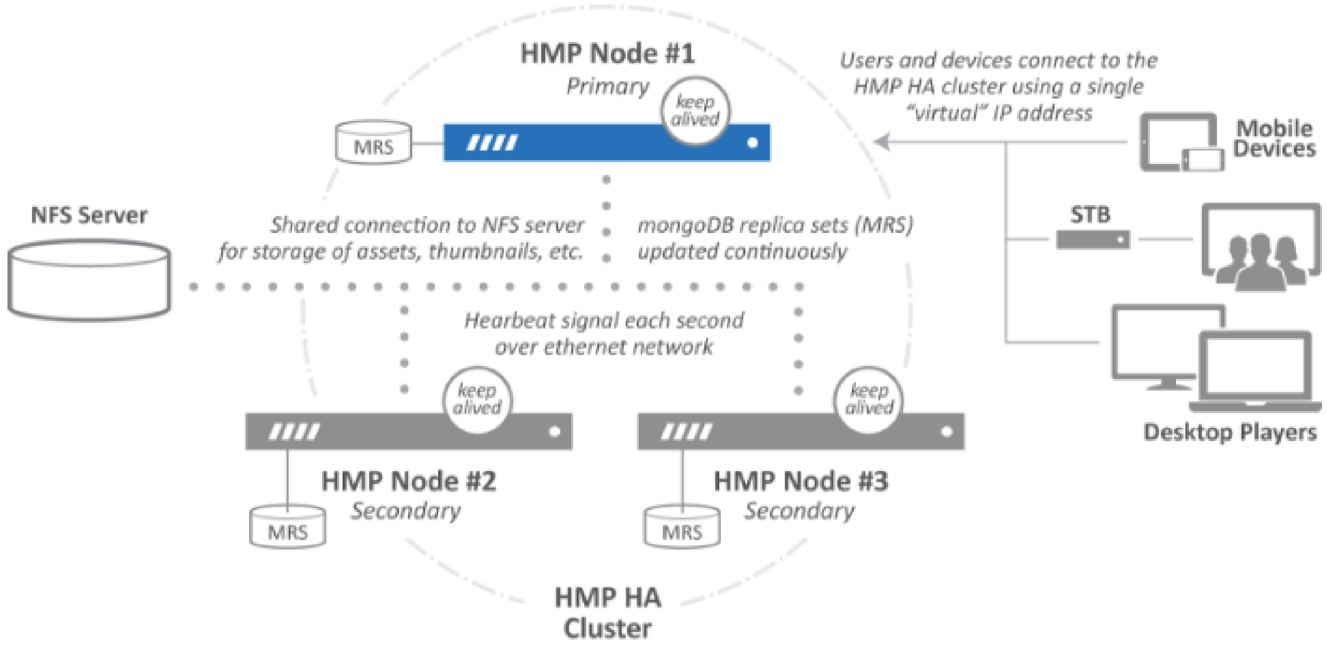
All HMP HA clusters must be implemented by Haivision Field Services.

**Available for existing HMP servers on 3.0, 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).**

**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.**


HMP Node #1
Primary
keep alived
MRS
Users and devices connect to the HMP HA cluster using a single "virtual" IP address
Mobile Devices
NFS Server
Shared connection to NFS server for storage of assets, thumbnails, etc.
mongoDB replica sets (MRS) updated continuously
STB
Hearbeat signal each second over ethernet network
keep alived
keep alived
HMP Node #2
Secondary
MRS
HMP Node #3
Secondary
MRS
Desktop Players
HMP HA Cluster

For more information, see the Haivision Support Portal.

**Related Topics**

- Viewing High Availability Cluster Status

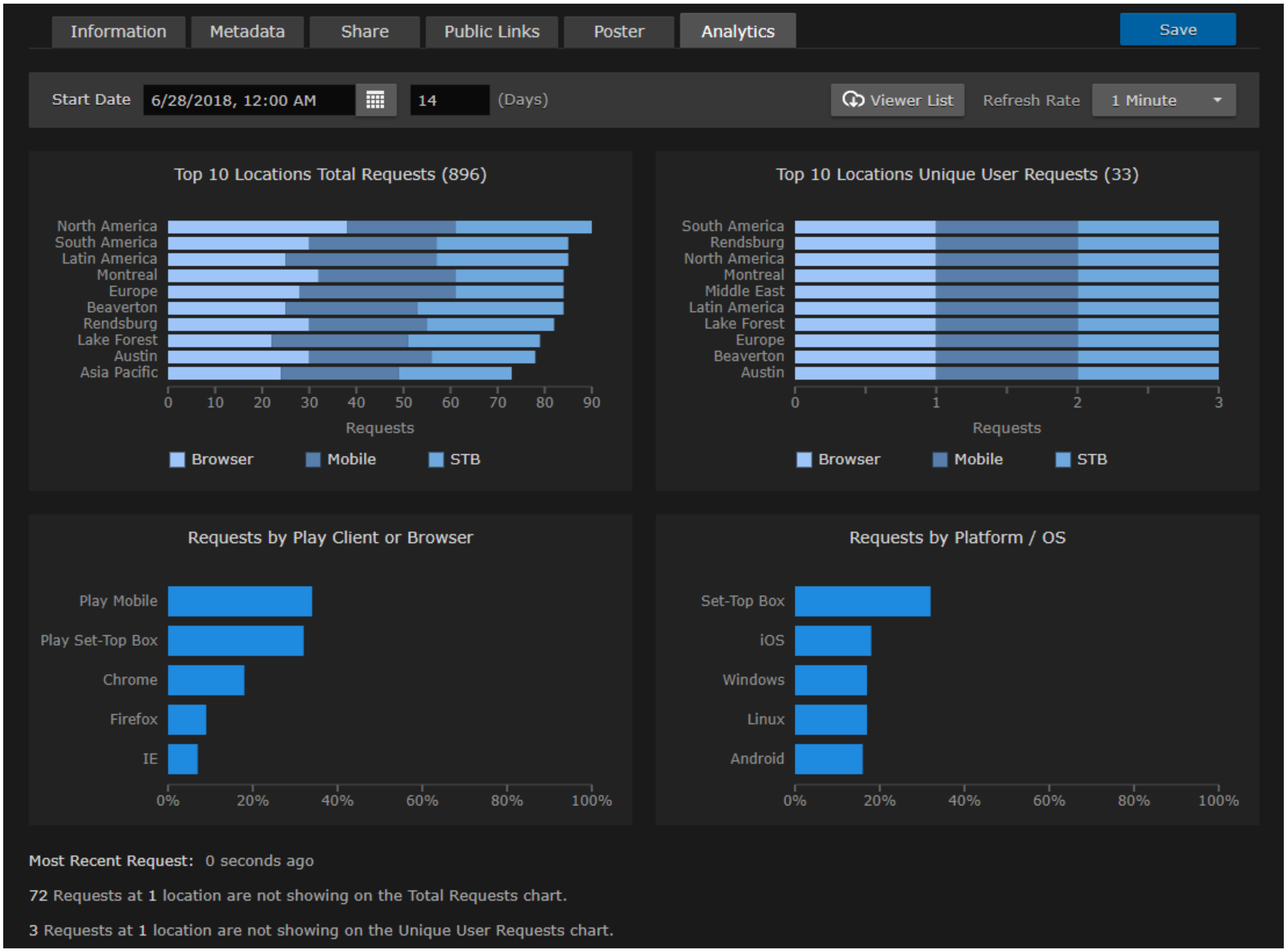
## Reporting and Analytics

In HMP 3.0, depending upon your permissions, you can view data about how viewers are interacting with your content as well as who is interacting with it.

Available metrics include the following:

- Number of views and unique viewers by location.
- Types of devices, browsers, and operating systems being used.

An Analytics tab is now available when you select a video, session, or source from the Content Library screen. With access to the Analytics tab, content owners and authorized users can generate and export (as .csv) a list of unique viewers and total requests.



Start Date 6/28/2018, 12:00 AM 14 (Days)

Refresh Rate 1 Minute

**Most Recent Request:** 0 seconds ago

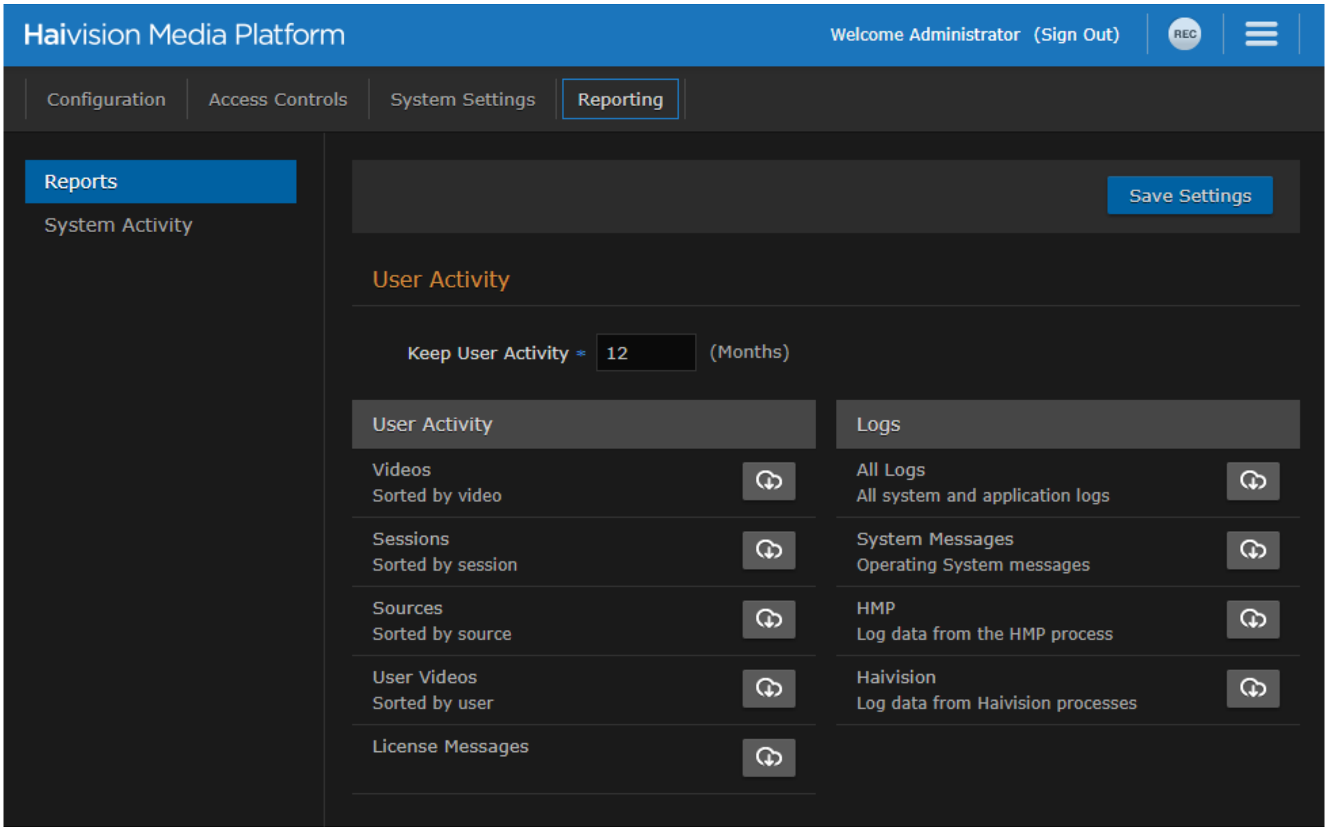
72 Requests at 1 location are not showing on the Total Requests chart.

3 Requests at 1 location are not showing on the Unique User Requests chart.

**Caution**

Usage records are stored in an internal database. If the Analytics page is displayed with hundreds of thousands of requests for the specified asset, HMP performance may be negatively impacted as these requests are being queried to be displayed.

**From the Reports page, administrators can continue to download system-wide user activity and logs as .csv files. User activities include watch, edit and delete entries while logs consist of system and application messages.**



User Activity

Keep User Activity * 12 (Months)

| User Activity | | Logs | |
|---|---|---|---|
| Videos<br>Sorted by video | | All Logs<br>All system and application logs | |
| Sessions<br>Sorted by session | | System Messages<br>Operating System messages | |
| Sources<br>Sorted by source | | HMP<br>Log data from the HMP process | |
| User Videos<br>Sorted by user | | Haivision<br>Log data from Haivision processes | |
| License Messages | | | |

To set analytics permissions for users, see Editing Role Permissions.

### Related Topics

- Collecting User Data Analytics for a Session (in the User's Guide)
- Collecting User Data Analytics for a Video (in the User's Guide)
- Reporting

## Physical Description (Servers)

Your Haivision Media Platform server comes delivered as enterprise-ready, ultra-compact appliance (either 1U or 2U) made for single-tier architectures.

**1U System** 2U System

***Haivision Media Platform 1U System***

- 25/50 or 50/100 Mbps recording/playback
- Active Directory support
- approximately 5 to 10 HD sources simultaneously (expandable)
- 1.8 TB RAID storage.

1U System **2U System**

***Haivision Media Platform 2U System***

- 50/100 to 200/400 Mbps recording/playback
- Active Directory support
- approximately 10 to 40 HD sources simultaneously (expandable)
- 6.6 TB RAID storage.

HMP servers provide either two or four 1 Gb Ethernet (GbE) Network Interface Card (NIC) ports for both traffic and management.

- 1U system: two ports
- 2U system: four ports

**Note**

For the system interfaces and LED status indicators, as well as instructions to install and connect to your server, please refer to the **Server Quick Start Guide - Issue 01**.

# Getting Started

**Important**

Before proceeding, make sure 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 - Issue 01**. 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

**Note**

Your browser may need to be Flash-enabled in order to use this site. System Administrators can set desktop browser playback to either the "Modern" HTML5 (via HLS) or "Legacy" Flash-based player. Both newly installed systems, as well as system upgrades default to the "Legacy" Player. For more information, see **Managing Security**.

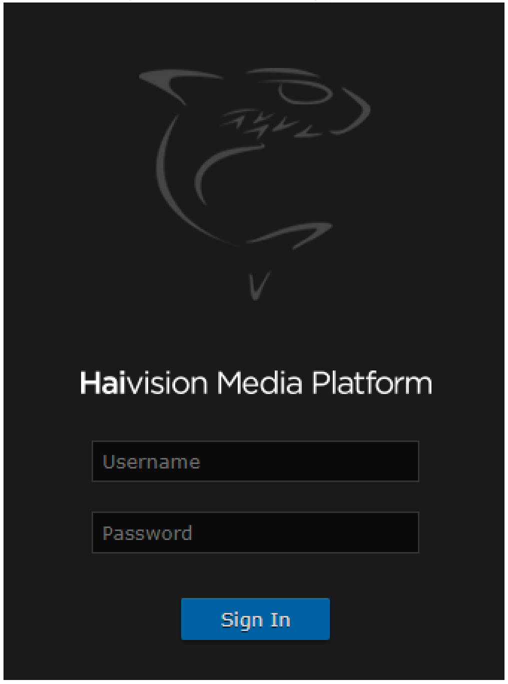
**To access the Haivision Media Platform Web interface:**

1. Open a Web browser of your choice, such as Chrome, Firefox, Safari, Microsoft Edge, or Internet Explorer (IE11).
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, you will see a Security Certificate warning. In this case, refer to **SSL Encryption** for details on how to supply HMP with an SSL security certificate in order to continue to the Sign-in screen.

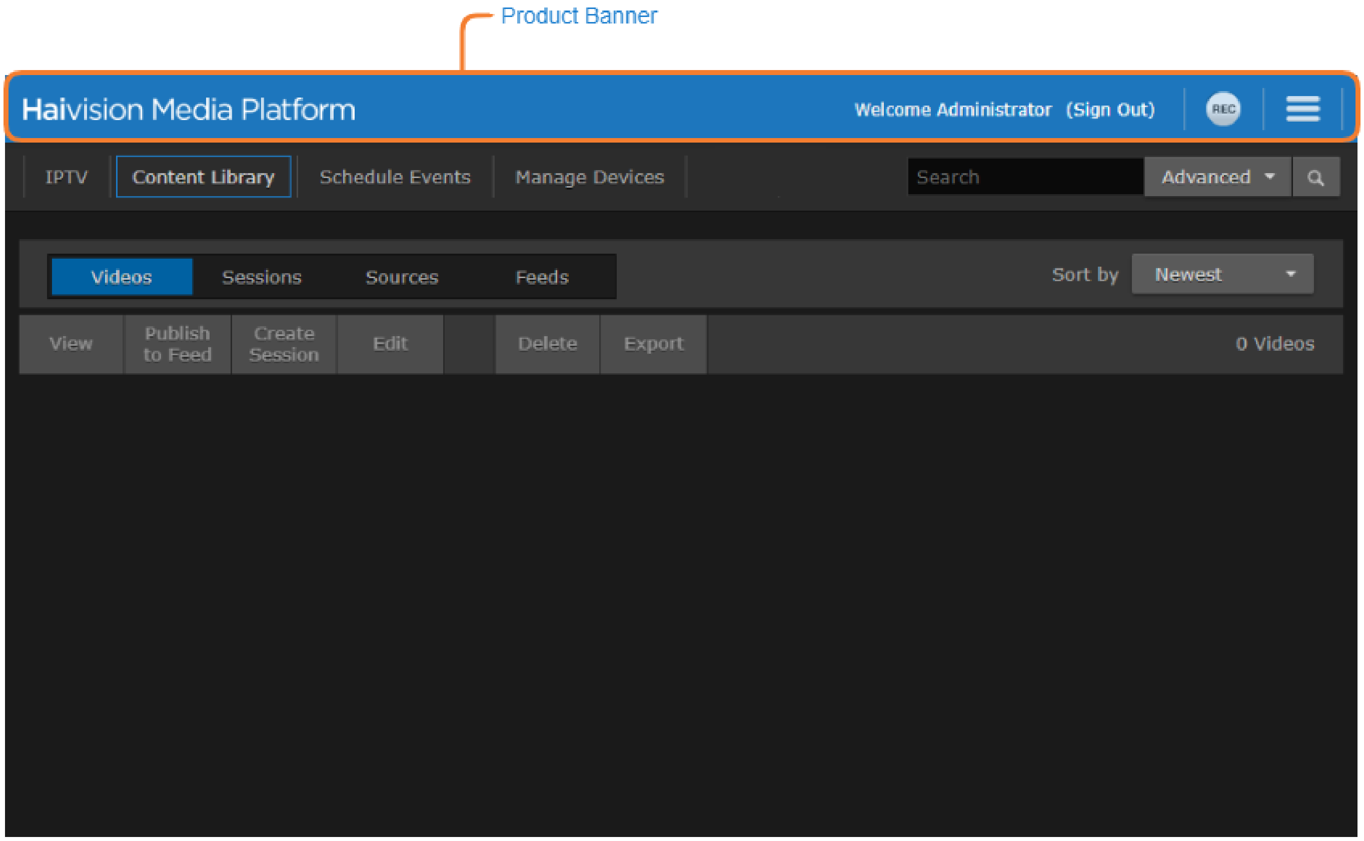
3. On the Sign-in screen, type the Username and Password and click **Sign In** (or press **Enter**).



**Important**

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**).

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



**Caution**

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

**Important**

`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, you are strongly advised to create a regular administrative user with a secure password.
To change the current user password, click the user name on the banner (next to "Welcome"). For details, see Changing the Default Password.

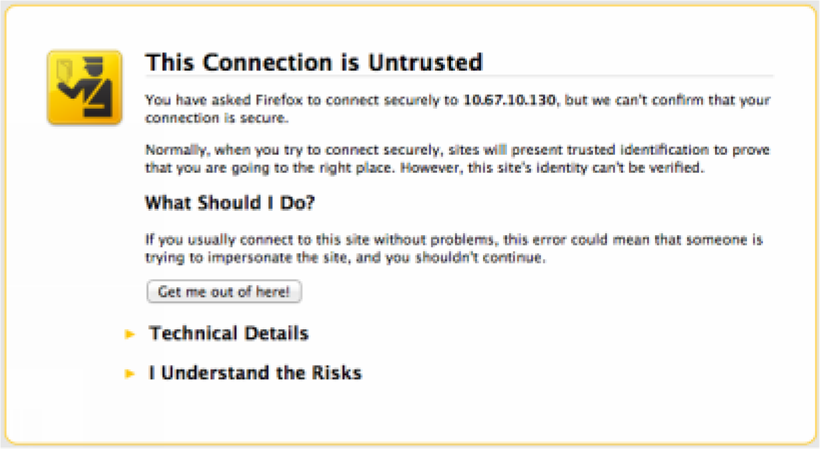
### Related Topics

- 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. When a browser accesses the website, it 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.



This Connection is Untrusted

You have asked Firefox to connect securely to **10.67.10.130**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

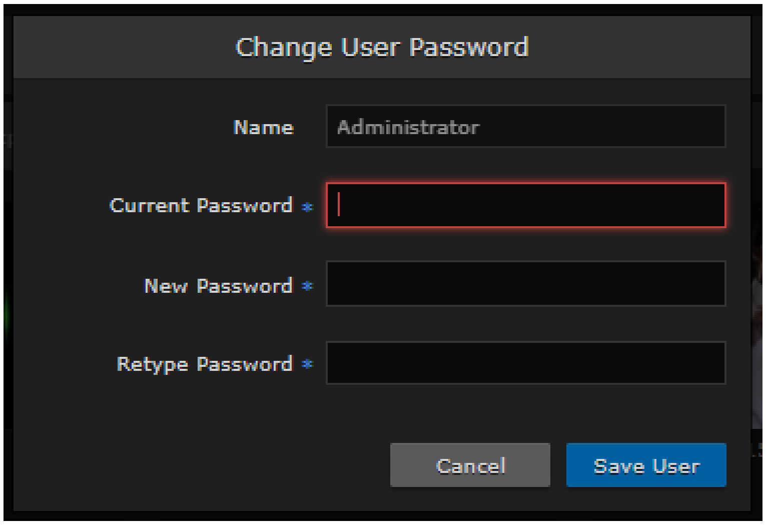
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

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

**To change the password for the current user:**

1. Click the user name (e.g., Administrator) on the toolbar (next to "Welcome").
2. On the Change User Password dialog, type your current password in the Current Password field.



Change User Password

Name: Administrator

Current Password *

New Password *

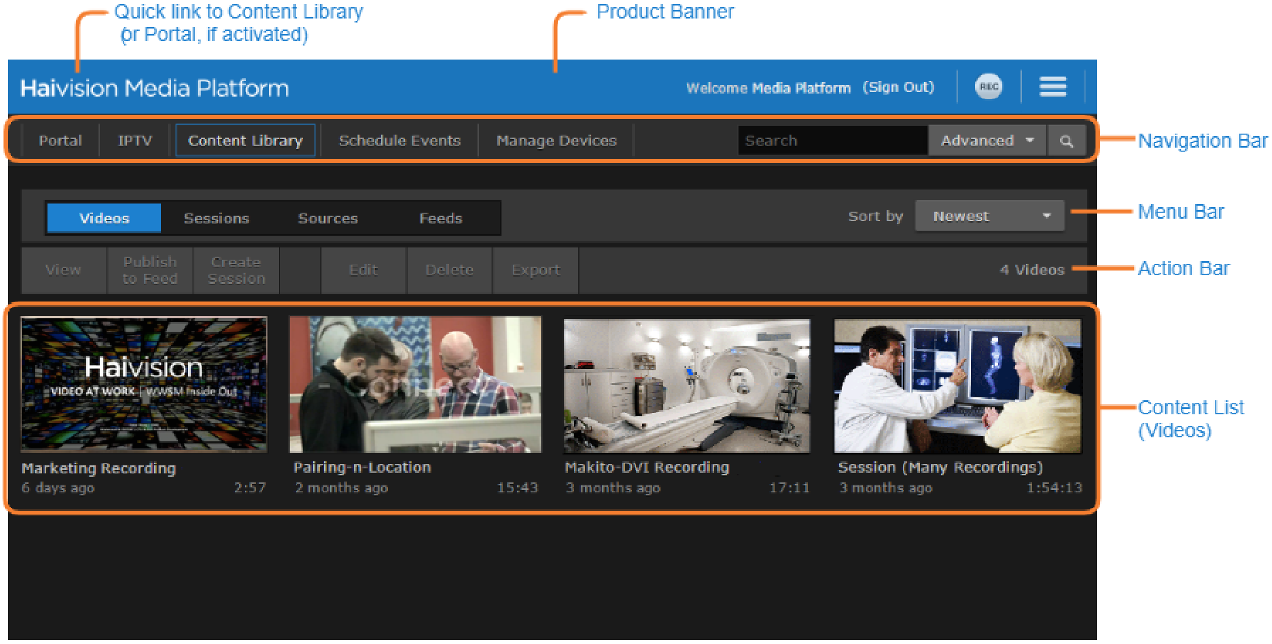
Retype Password *

3. Type the new password in the New Password field and again in the Retype Password field.
4. Click **Save User**.
   The password change will take effect immediately.

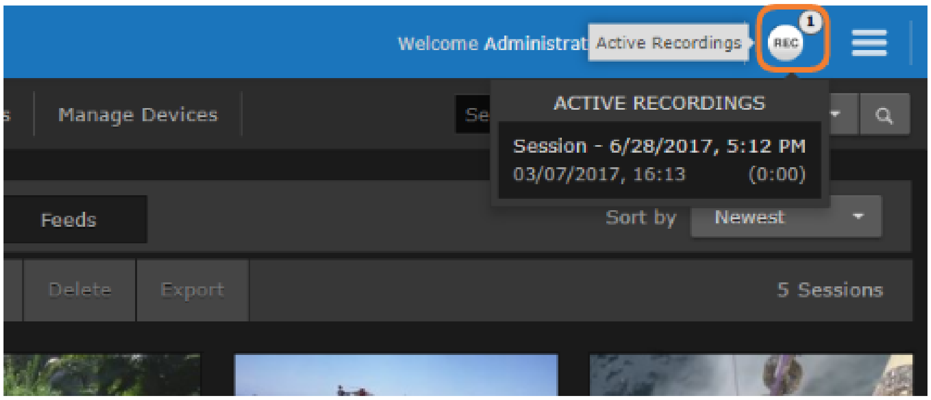
## Navigating the Interface

When you first sign in, the Haivision Media Platform Web interface opens to the Content Library (showing the Videos list, as shown in the following example).

- If you activate the Portal, the Web 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**.
- If EPG is licensed on your system, the IPTV link will show on the navigation bar.



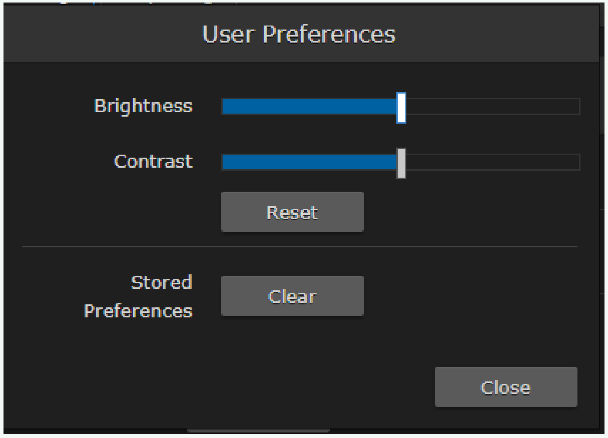
- To open the Portal, view live IPTV content, schedule an event, or manage set-top boxes, click the option on the navigation bar.  Clicking an option opens the selected screen.
- To view a list of active recordings, click the REC icon on the product banner. Clicking on a recording in the list takes you to the Viewer for that recording.



- To navigate the Administration or Import/Export screen, click the ☰ icon on the banner and select from the navigation drop-down menu.

**Tip**

To display a list of new HMP features, select **What's New** from the navigation drop-down menu.
To adjust the brightness and contrast, or reset the HMP stored preferences, select **User Preferences** from the navigation drop-down menu.



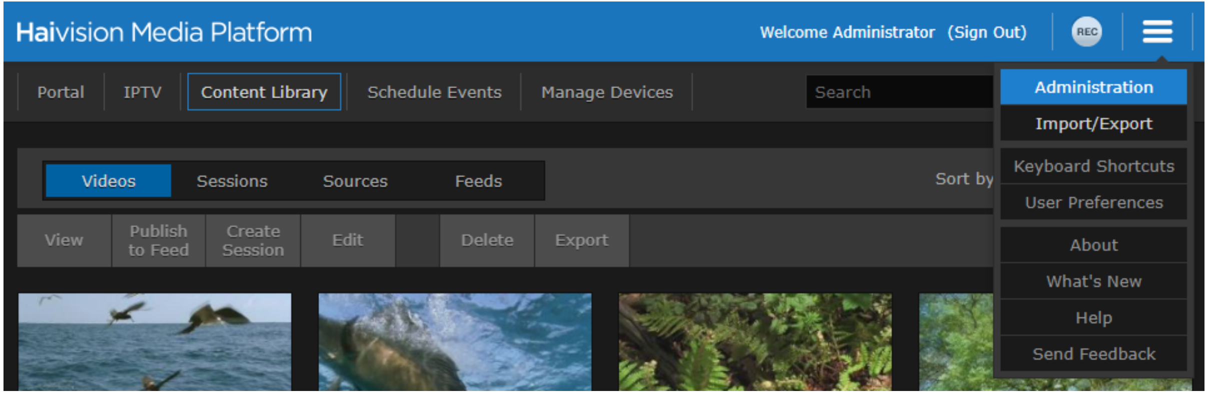
After successfully signing in, system integrators and administrators will need to go to the Administration screen (see Configuring HMP.)
For an overview of the Web interface, including viewing and search options, see the User's Guide.

## Modifying the IP Address

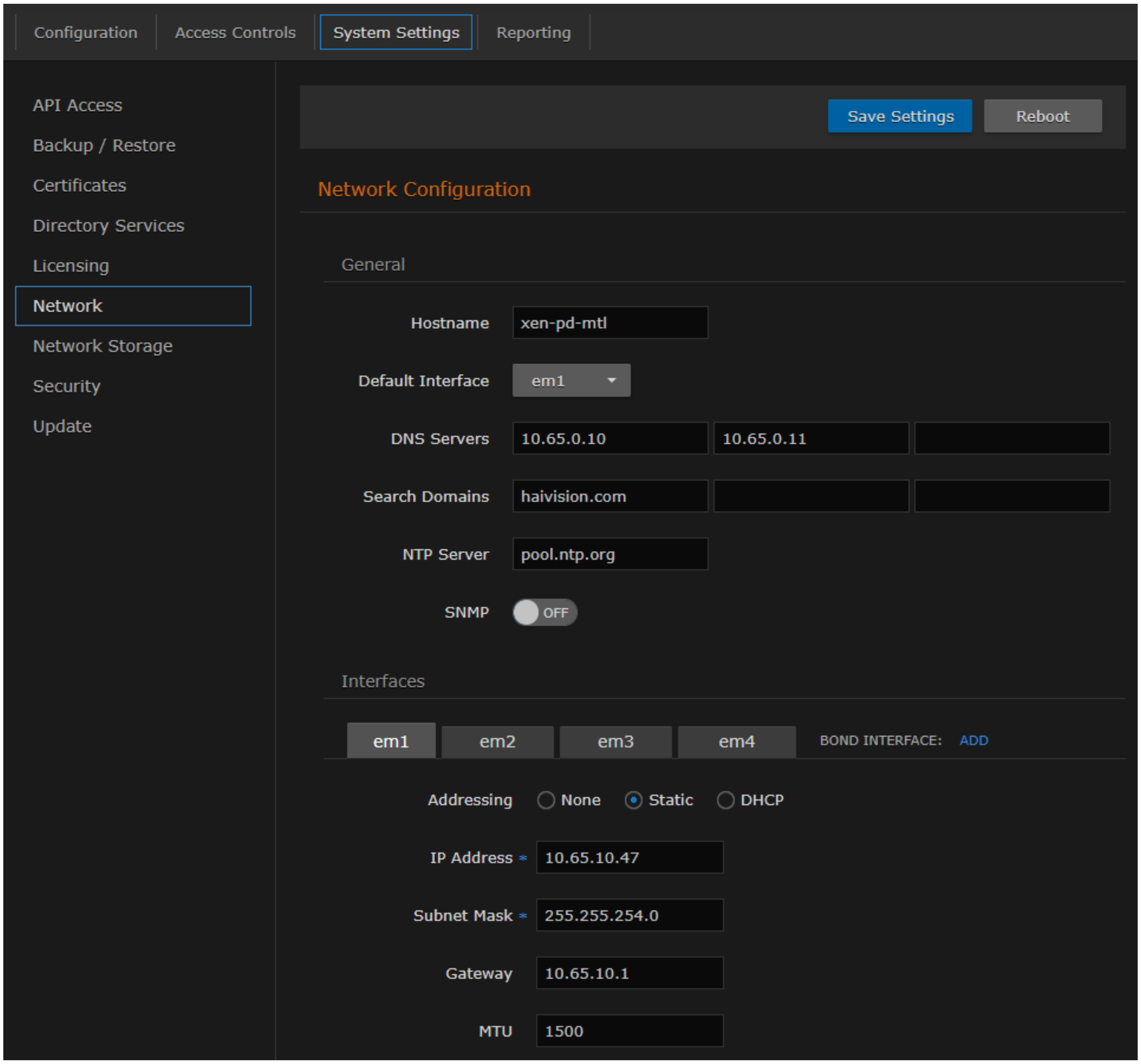
**Tip**

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 - Issue 01). 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.



Network Configuration

General

Hostname: xen-pd-mtl

Default Interface: em1

DNS Servers: 10.65.0.10 | 10.65.0.11

Search Domains: haivision.com

NTP Server: pool.ntp.org

SNMP: OFF

Interfaces

em1 | em2 | em3 | em4 | BOND INTERFACE: ADD

Addressing: ○ None ● Static ○ DHCP

IP Address *: 10.65.10.47

Subnet Mask *: 255.255.254.0

Gateway: 10.65.10.1

MTU: 1500

3. On the Network Configuration page, for the first network interface ( `em1` in the above example), either:

- Select DHCP to enable Dynamic Host Configuration Protocol,
  -or-
- Enter a valid IP address, subnet mask, and gateway to work in your environment.

4. Click **Save Settings**, and then click **Reboot**.
5. After the system has rebooted, sign in again to continue.

## Basic Actions

This section shows how to perform editing and deleting tasks that recur throughout HMP configuration and administration. These tasks may be applied to items such as feeds, locations, and sources on the Administration screens.

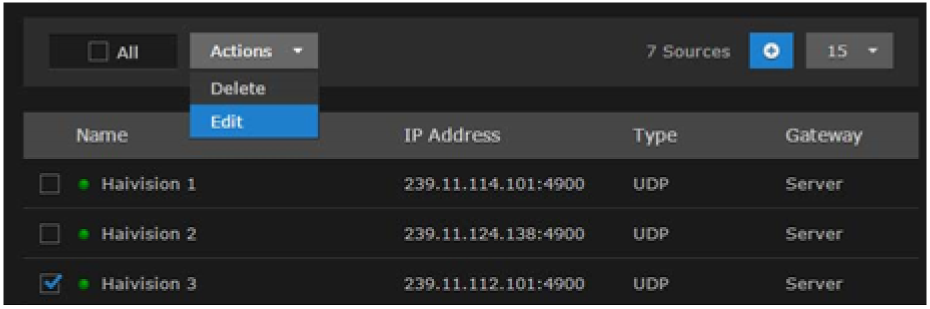
**Topics Discussed**

- **Editing Items**
- **Deleting Items**

## Editing Items

To edit items:

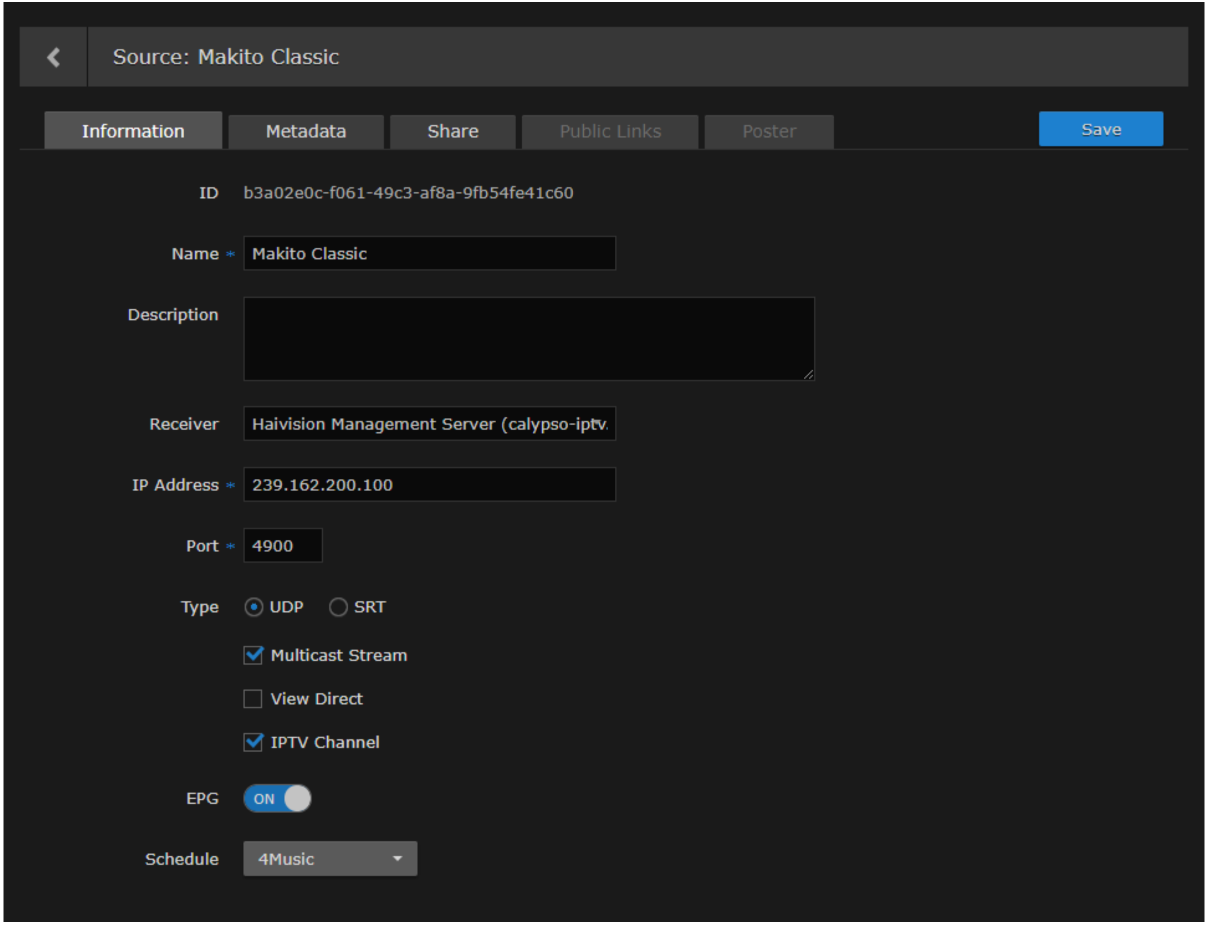
1. On a list, such as the Administration Sources list, click anywhere on the item's row to edit it.
   -or-
   Check the checkbox next to one or more items (or check All), and select **Edit** from the Actions drop-down menu.



| | Name | IP Address | Type | Gateway |
|---|---|---|---|---|
| ☐ | ● Haivision 1 | 239.11.114.101:4900 | UDP | Server |
| ☐ | ● Haivision 2 | 239.11.124.138:4900 | UDP | Server |
| ☑ | ● Haivision 3 | 239.11.112.101:4900 | UDP | Server |

> **Note**
>
> If you select multiple items, in some cases, the Edit menu option is not available, or the Information pane contains only a limited subset of values, such as the Description.

Selecting an item from the list opens the Information pane. For example:



ID b3a02e0c-f061-49c3-af8a-9fb54fe41c60

Name * Makito Classic

Description

Receiver Haivision Management Server (calypso-iptv.

IP Address * 239.162.200.100

Port * 4900

Type ● UDP ○ SRT

☑ Multicast Stream

☐ View Direct

☑ IPTV Channel

EPG ON

Schedule 4Music ▾

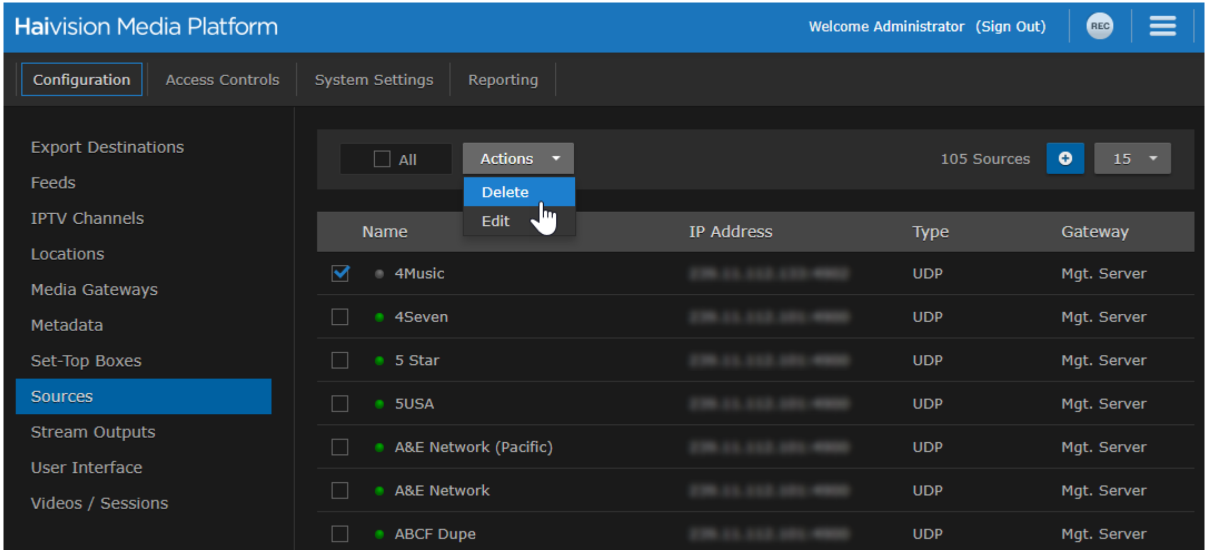
2. On the Information pane, enter or select the values to modify the item.
3. Click **Save**.
4. To assign metadata to the item (where applicable), click the **Metadata** tab. For details, see Configuring Sources to assign metadata to sources, or the User's Guide to edit metadata for sessions and videos.
5. To share the item, click the **Share** tab. For details, see Sharing Items (in the User's Guide).

> **Tip**
>
> When editing sessions (Content Library screen), you can also define Public Links. To do so, click the **Public Links** tab. For details, see the User's Guide.

## Deleting Items

To delete items:

1. On a list such as the Administration Sources list (example shown below), check the checkbox next to one or more items in the list (or check **All**).
2. Select **Delete** from the Actions drop-down menu.



| | Name | IP Address | Type | Gateway |
|---|---|---|---|---|
| ☑ | 4Music | [redacted] | UDP | Mgt. Server |
| ☐ | 4Seven | [redacted] | UDP | Mgt. Server |
| ☐ | 5 Star | [redacted] | UDP | Mgt. Server |
| ☐ | 5USA | [redacted] | UDP | Mgt. Server |
| ☐ | A&E Network (Pacific) | [redacted] | UDP | Mgt. Server |
| ☐ | A&E Network | [redacted] | UDP | Mgt. Server |
| ☐ | ABCF Dupe | [redacted] | UDP | Mgt. Server |

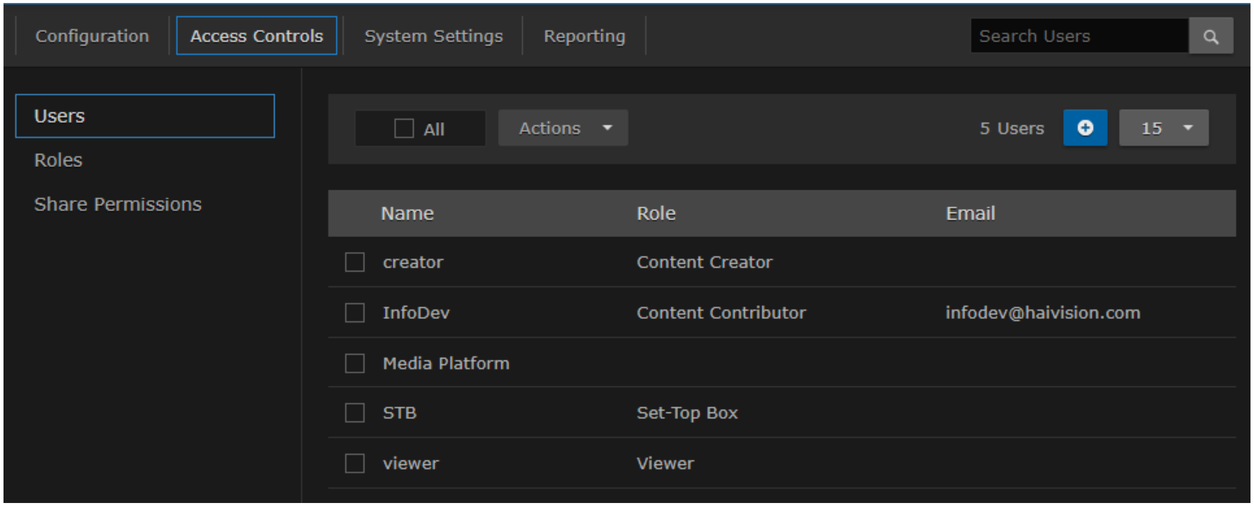
3. Click **Confirm** (or where applicable, select **Delete** from the warning dialog).

The selected item(s) will be removed from the list.

## Creating a New Admin User

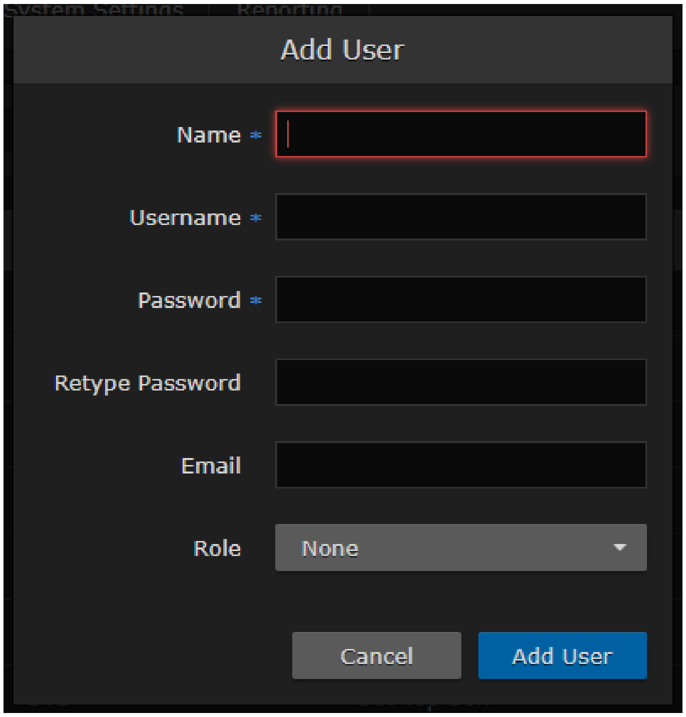
Follow these steps to create a new administrative user from the Web Interface.

1. On the Administration page, click **Access Controls** on the toolbar and then click **Users** on the sidebar.
2. From the Users list, click the ⊕ icon.



| | Name | Role | Email |
|---|---|---|---|
| □ | creator | Content Creator | |
| □ | InfoDev | Content Contributor | infodev@haivision.com |
| □ | Media Platform | | |
| □ | STB | Set-Top Box | |
| □ | viewer | Viewer | |

3. On the Add User dialog, enter the display Name, Username/Password for logging in, and Email address to associate with the user account.



4. **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 in order to log in. Users may also be assigned “share” permissions for content rights (recordings and sessions) by administrators or other users.

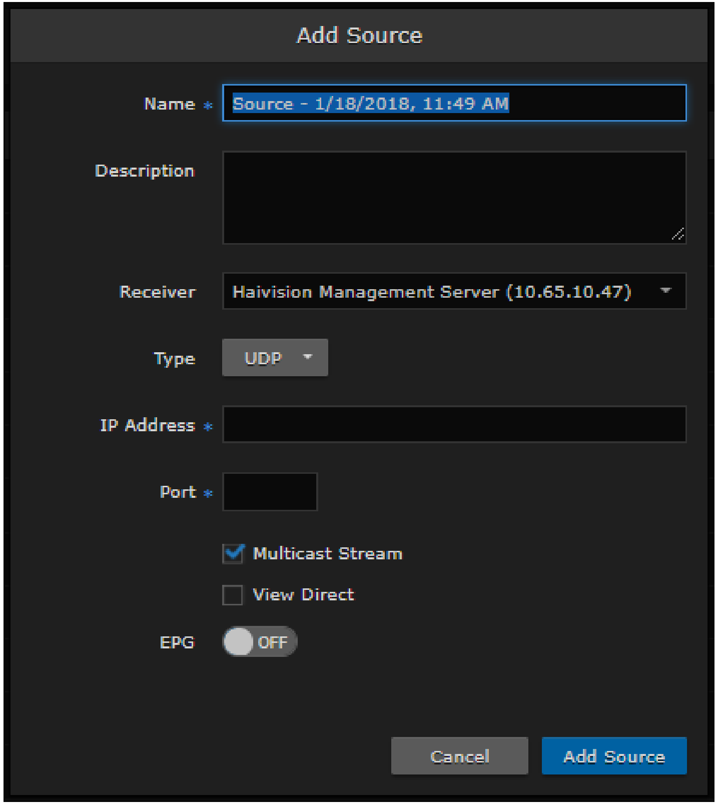
5. Click **Add User**.
   The new user will be added to the Users list.
6. Click **Sign Out** on the navigation bar and then sign in with your new credentials to have full administrative permissions.

> **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.

1. On the Administration page, click **Configuration** on the toolbar and then click **Sources** on the sidebar.
2. From the Sources list, click the ⊕ icon.
3. On the Add Source dialog, enter the Name, Description, IP Address, and Port for the source. Leave the default Type (UDP) and Receiver (HMP).



Name * Source - 1/18/2018, 11:49 AM

Description

Receiver Haivision Management Server (10.65.10.47)

Type UDP

IP Address *

Port *

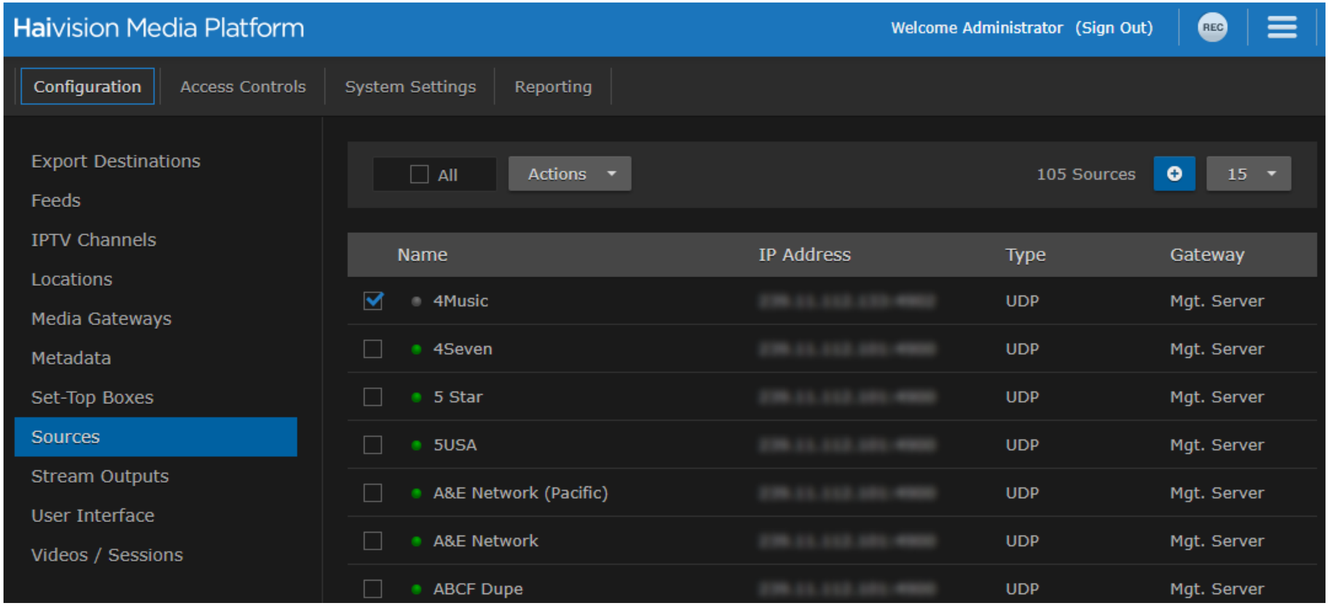
☑ Multicast Stream

☐ View Direct

EPG OFF

4. For a unicast stream, uncheck the Multicast Stream checkbox.
5. To configure the source as an IPTV channel (available for viewing from a Haivision Play Set-Top Box), check the IPTV checkbox.
6. 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.)

7. Click **Add Source**.
   The new source will be added to the Sources list (example shown following).



|  | Name | IP Address | Type | Gateway |
|---|---|---|---|---|
| ☑ | ● 4Music | [redacted] | UDP | Mgt. Server |
| □ | ● 4Seven | [redacted] | UDP | Mgt. Server |
| □ | ● 5 Star | [redacted] | UDP | Mgt. Server |
| □ | ● 5USA | [redacted] | UDP | Mgt. Server |
| □ | ● A&E Network (Pacific) | [redacted] | UDP | Mgt. Server |
| □ | ● A&E Network | [redacted] | UDP | Mgt. Server |
| □ | ● ABCF Dupe | [redacted] | UDP | Mgt. Server |

Once 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 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 Installation Guide**.

### 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**

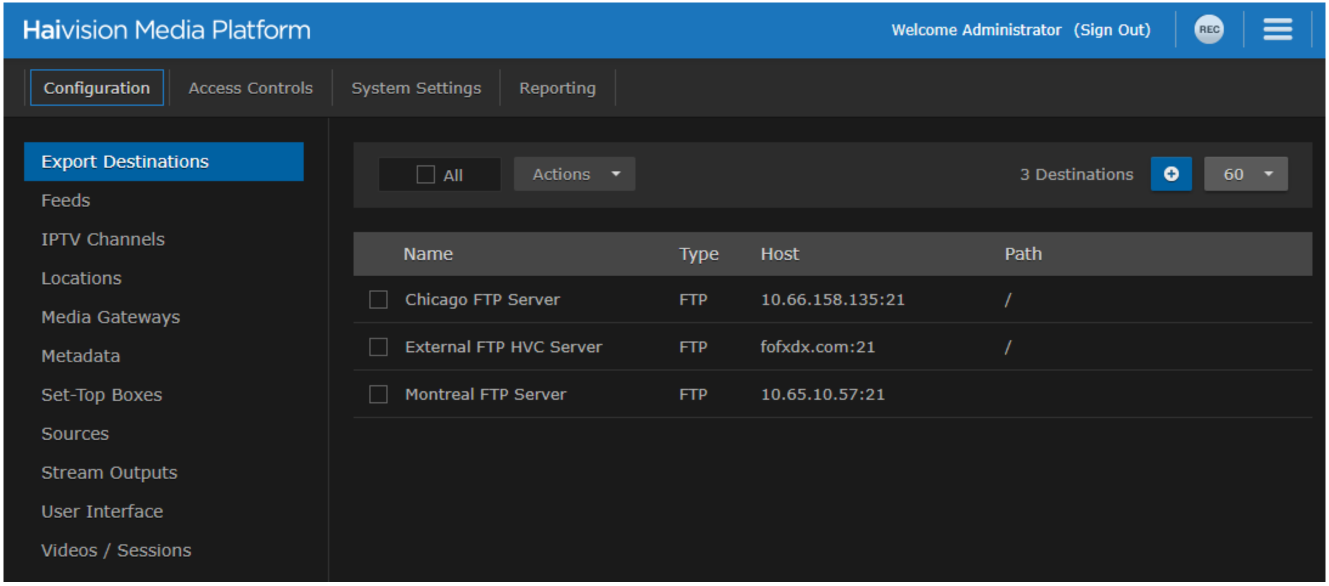
## Configuring Export Destinations

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.

These destinations will be available for users to select when exporting videos. For more information, see **Managing Exports** (in the **User's Guide**).

To view and manage the export destinations:

1. To navigate the Administration screen, click the ☰ icon on the banner and select **Administration** from the navigation drop-down menu.
2. On the Administration screen, 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 (see following example).

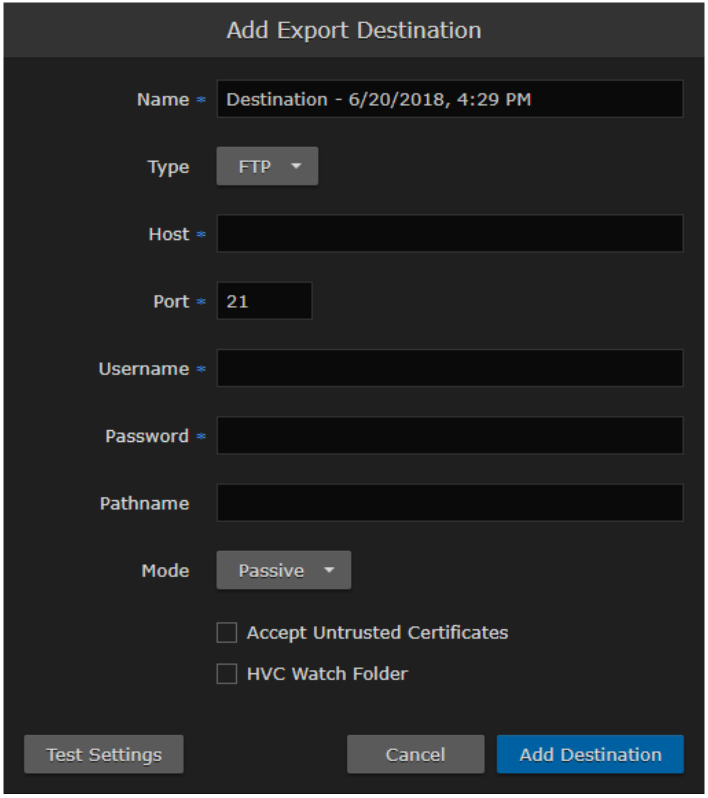


| | Name | Type | Host | Path |
|---|---|---|---|---|
| □ | Chicago FTP Server | FTP | 10.66.158.135:21 | / |
| □ | External FTP HVC Server | FTP | fofxdx.com:21 | / |
| □ | Montreal FTP Server | FTP | 10.65.10.57:21 | |

To add an export destination:

1. From the Export Destinations pane, click the ⊕ icon.

2. On the Add Export Destination dialog, type in a name and enter or select the value(s) to define the destination. See Export Destination Settings.



Add Export Destination

Name * Destination - 6/20/2018, 4:29 PM

Type FTP

Host *

Port * 21

Username *

Password *

Pathname

Mode Passive

□ Accept Untrusted Certificates

□ HVC Watch Folder

3. To test the connection, click **Test Settings**.

> **Note**
>
> You do not need to save in order to test settings.

4. Click **Add Destination**. The new export destination will be added to the list.

### Related Topics

- Export Destination Settings

## Export Destination Settings

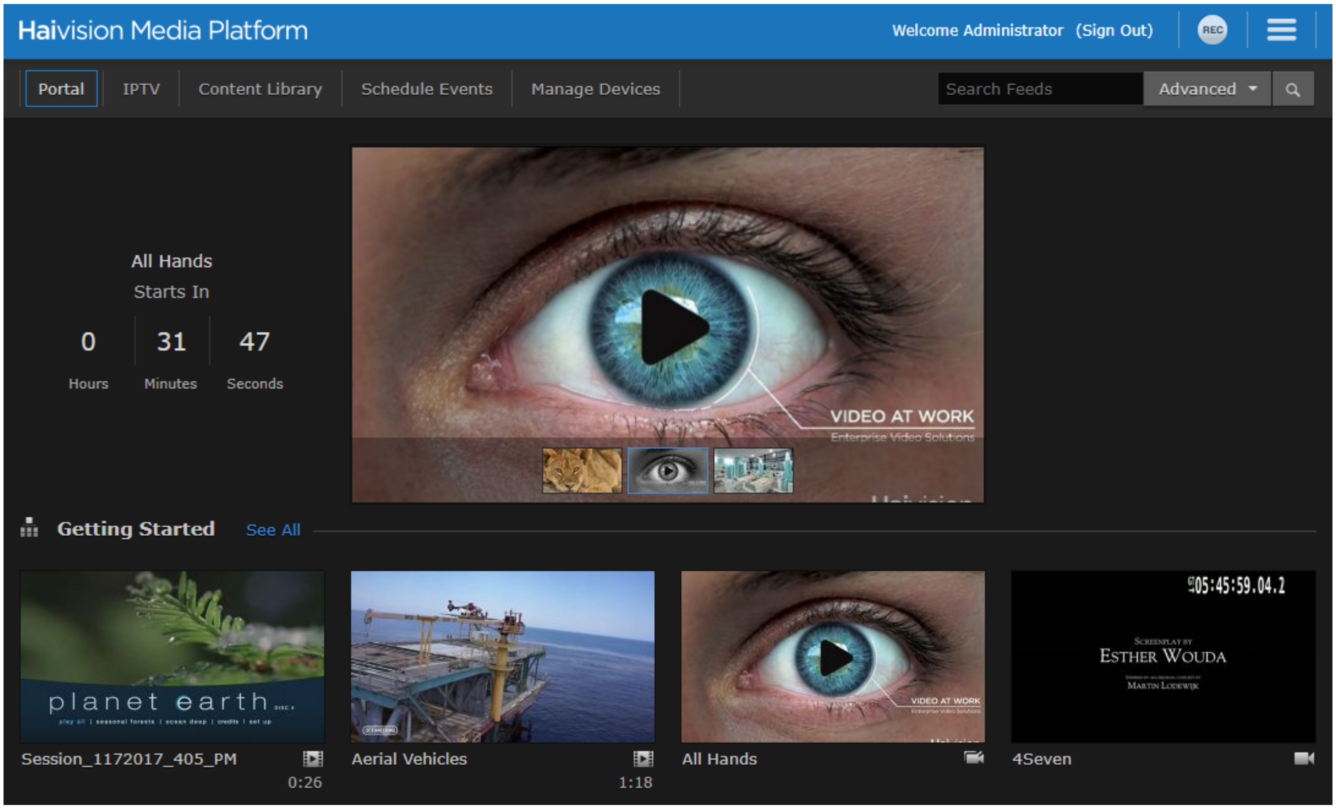
The following table lists the Export Destination configuration settings:

| Setting | Default | Description/Values |
|---|---|---|
| Name | n/a | Enter a name for the destination. This name will be selectable on the Export Video list. |
| Type | FTP | Select the protocol type, either:<br>• FTP: File Transfer Protocol<br>• FTPS: FTP with explicit Transport Layer Security (TLS) |
| Host | n/a | Type in the server’s DNS host name or IP address for the destination. |
| Port | 21 | Type in the port number for the destination server. |
| Username | n/a | Type in your login username for the site. |
| Password | n/a | Type in your password. |
| Pathname | n/a | (Optional) Type in the 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, either:<br>• 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.<br>• 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 | **Note**<br>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. |

# 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 thing users see when they sign into HMP.



From the Portal, viewers can browse feeds, search for items, and launch the video, session, or source in a default viewer. For the Portal user workflow, see Exploring the Web Interface (in the User's Guide).

From the Feeds pane, administrators can create, share, and manage Portal feeds, including turning the Portal on and off.

Once the Portal is turned on, content managers can populate the feeds and promote items to "Suggested" and "Featured" using the (Content Library) Feeds editor. For details, see Managing Feeds (in the User's Guide).

To view and manage video feeds:

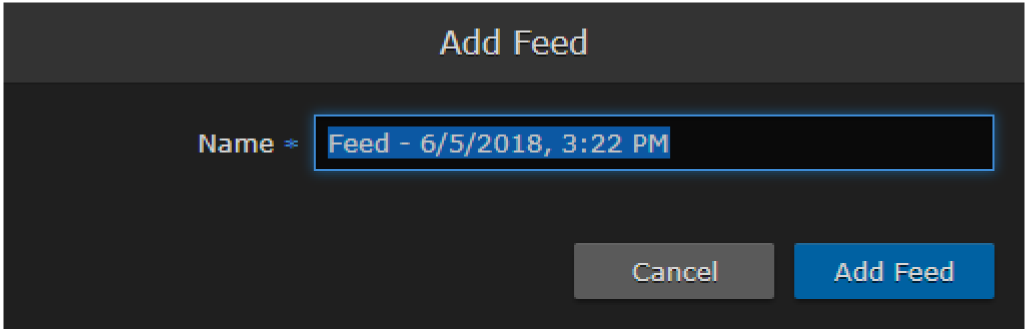
1. On the Administration screen, click **Configuration** on the toolbar and then **Feeds** on the sidebar. The Feeds pane opens, displaying the list of defined feeds, if any (see following example).
2. To activate the Portal, toggle the **Portal Access** button to **On**. The *Portal* option will be added to the navigation bar (next to Content Library).
3. To allow Feed permissions to take precedence over the Share 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 is not shared with them. However, the **Use Feed Permission** toggle option allows administrators to reverse this.
> This setting saves content managers from having to share all the individual items in feeds. Instead they simply share 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.



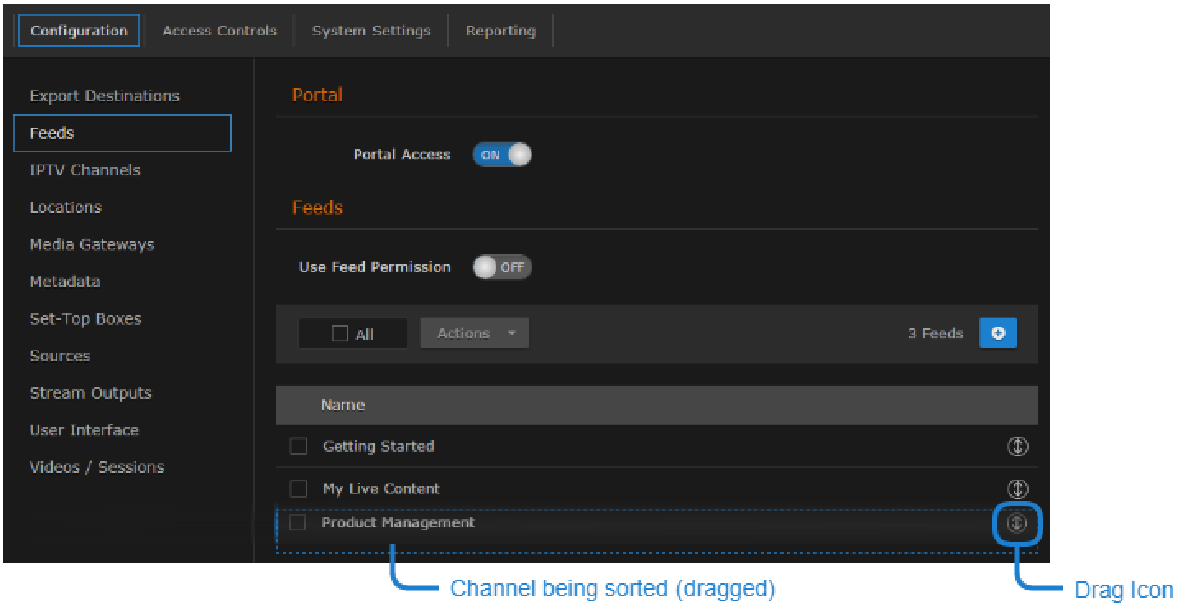
Add Feed

Name * Feed - 6/5/2018, 3:22 PM

3. Click **Add Feed**.
   The new feed will be added to the Feeds list.
4. To share a feed, select the feed from the list, and on the Information pane, click the **Share** tab. Follow the steps in **Sharing Items** (in the **User's Guide**).

> **Note**
>
> See the note in the previous section re: Feed Permissions.

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



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

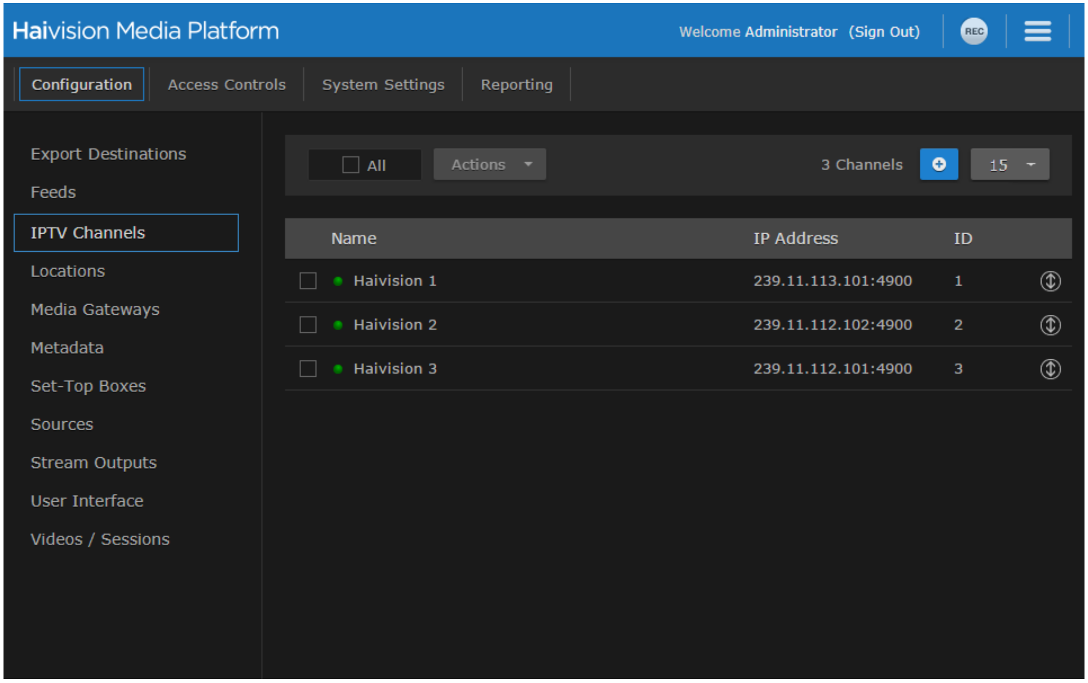
## Configuring IPTV Channels

IPTV channels are sources that have been enabled for IPTV deployment via Haivision Play Set-Top Boxes. You can set up IPTV channels and assign access from here or from the Sources pane.

To view and manage IPTV channels:

1. On the Administration screen, 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).



| Name | IP Address | ID |
|---|---|---|
| Haivision 1 | 239.11.113.101:4900 | 1 |
| Haivision 2 | 239.11.112.102:4900 | 2 |
| Haivision 3 | 239.11.112.101:4900 | 3 |

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. Type in a name and enter or select the value(s) to define the source. See **Source Settings**.
3. Click **Add Source**.
   The new source will be added to both the IPTV Channel and Sources lists.

## Configuring Locations

When setting up Haivision Media Platform, depending on the Product Edition, administrators can define additional site locations (for example, satellite offices). The purpose is to define networks on which users reside in order to route users through the closest 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 where the user is and where the closest streaming device is (i.e., Media Gateway).

**Note**

For more information on HMP-Media Gateway pairing, see **Configuring HMP-Media Gateway Pairings**. For details on Media Gateways, please refer to the Media Gateway **User's Guide** as well as the Haivision website at: **https://www.haivision.com**

- To view a listing of the incoming and outgoing links between the currently configured locations, see **Locations Topology**.
- To create Distribution Policies to manage live stream routes, see **Locations Policies**.

### Multicast Playback

With Multicast Support, HMP delivers multicast outputs from Media Gateway(s) directly to browsers running on users' desktops (PC/Mac) when the network supports multicast (MPEG2-TS).

**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**.

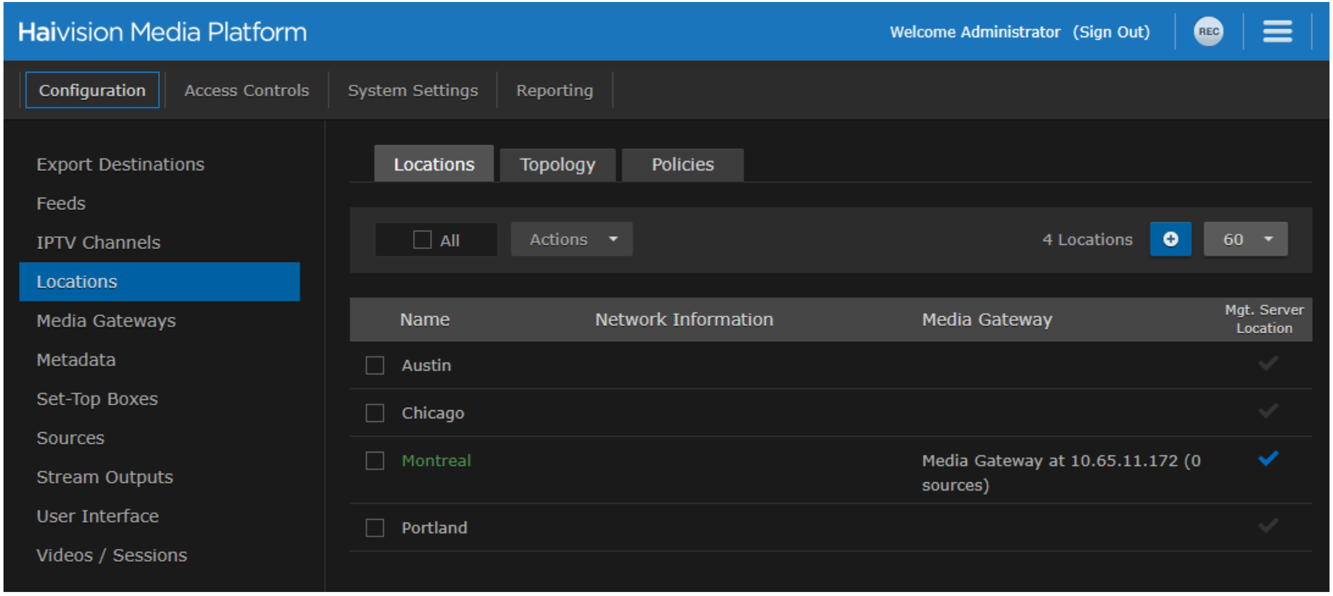
**Topics Discussed**

- **Managing Locations**
- **Troubleshooting Multicast & Diagnostic Tool**
- **Location Settings**
- **Locations Topology**
- **Locations Policies**

## Managing Locations

To view and manage locations:

1. On the Administration screen, click **Configuration** on the toolbar and then click **Locations** on the sidebar.
   The Locations pane opens, displaying the list of defined locations, if any (see following example).

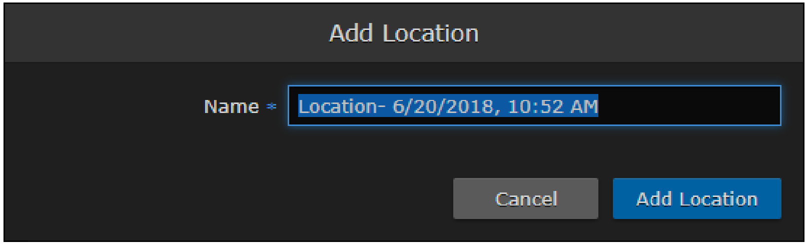


| | Name | Network Information | Media Gateway | Mgt. Server Location |
|---|---|---|---|---|
| □ | Austin | | | ✓ |
| □ | Chicago | | | ✓ |
| □ | Montreal | | Media Gateway at 10.65.11.172 (0 sources) | ✓ |
| □ | Portland | | | ✓ |

2. (If required) Check the checkbox under Mgt. Server Location to identify the location of the HMP management server.

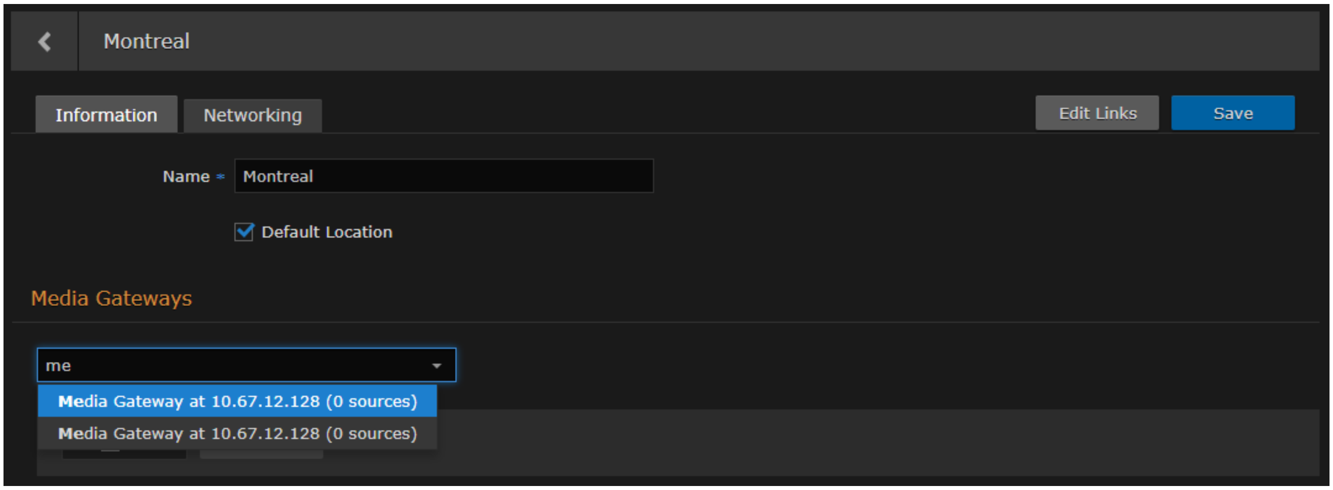
To add a site location:

1. From the Locations pane, click the ⊕ icon.
2. On the Add Location dialog, type the location name in the Name text field.



Name * Location- 6/20/2018, 10:52 AM

3. Click **Add Location**.
4. On the Location Information pane, you can edit the location name, set the Default Location (see Location Settings), and configure its list of gateways.
5. To select a gateway, type the first few characters of the gateway name in the Media Gateway field and then select the name from the auto-complete drop-down list of available paired gateways. See Configuring HMP-Media Gateway Pairings.



Name * Montreal

☑ Default Location

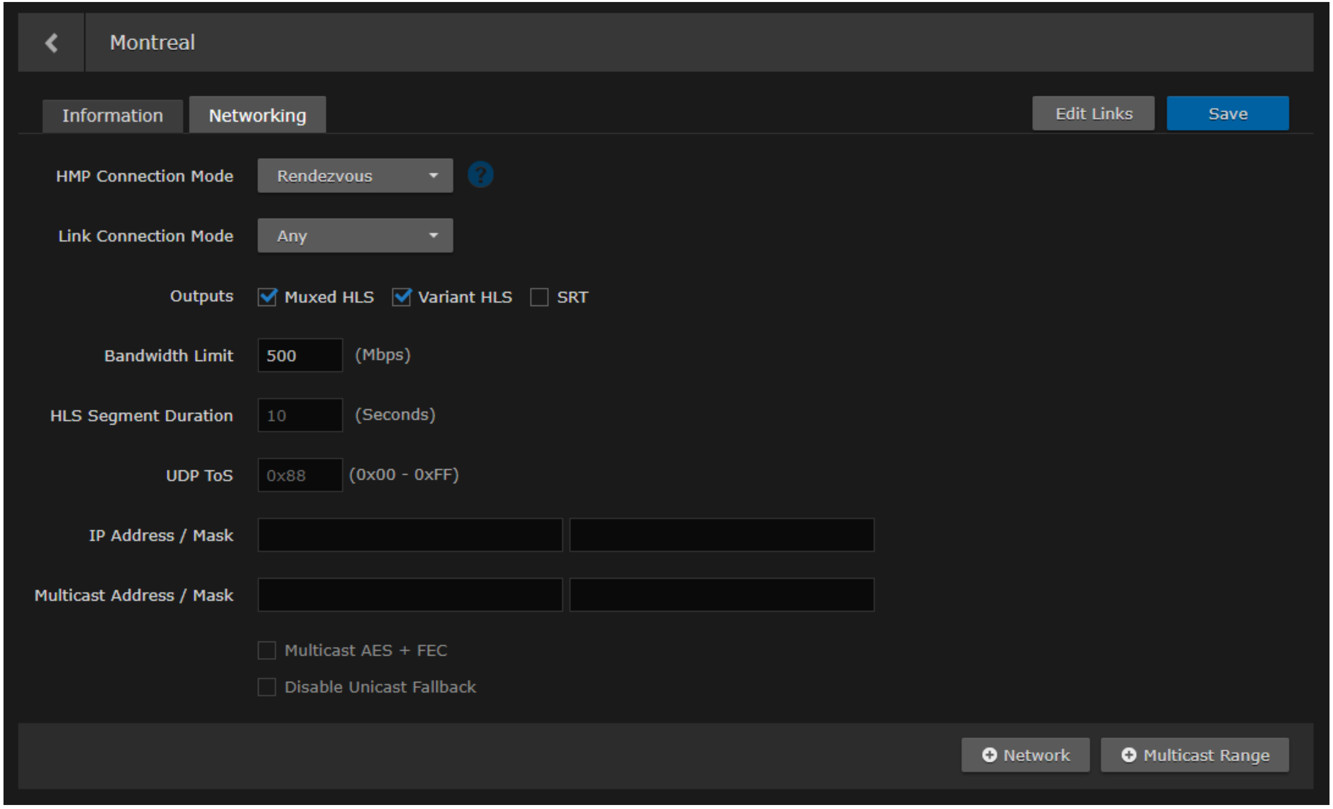
Media Gateways

me

Media Gateway at 10.67.12.128 (0 sources)
Media Gateway at 10.67.12.128 (0 sources)

The gateway is then added to the list.

6. To configure network settings as well as multicast playback, click the **Networking** tab and then fill in the fields to define the location. For details, see the "Networking" section of the table in Location Settings.



HMP Connection Mode: Rendezvous

Link Connection Mode: Any

Outputs: ☑ Muxed HLS ☑ Variant HLS □ SRT

Bandwidth Limit: 500 (Mbps)

HLS Segment Duration: 10 (Seconds)

UDP ToS: 0x88 (0x00 - 0xFF)

IP Address / Mask

Multicast Address / Mask

□ Multicast AES + FEC

□ Disable Unicast Fallback

7. To enable encrypted multicast (AES) for the location, check the Multicast AES + FEC checkbox.
8. To specify additional multicast addresses and subnet masks for the location, click **+Multicast Range**.
9. To specify additional IP addresses and subnet masks for the location, click **+Network**.

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

10. Click **Save**.

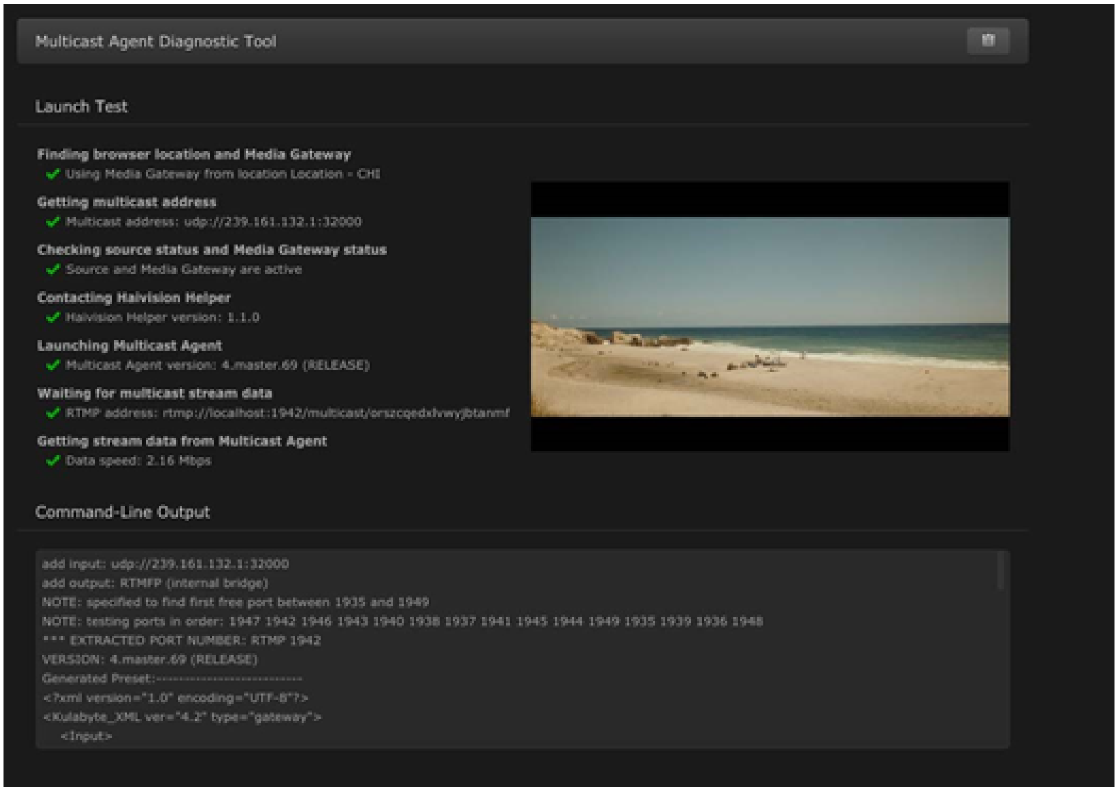
## Troubleshooting Multicast & Diagnostic Tool

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

- Are HMP and the Gateway(s) 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.
- Choose "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 will cause the tool to open in a new tab. Tests done by the diagnostic tool will use the source that was in the player that was clicked in this way.



Multicast Agent Diagnostic Tool

Launch Test

**Finding browser location and Media Gateway**
✓ Using Media Gateway from location Location - CHI

**Getting multicast address**
✓ Multicast address: udp://239.161.132.1:32000

**Checking source status and Media Gateway status**
✓ Source and Media Gateway are active

**Contacting Haivision Helper**
✓ Haivision Helper version: 1.1.0

**Launching Multicast Agent**
✓ Multicast Agent version: 4.master.69 (RELEASE)

**Waiting for multicast stream data**
✓ RTMP address: rtmp://localhost:1942/multicast/orszcqedxlvwyjbtanmf

**Getting stream data from Multicast Agent**
✓ Data speed: 2.16 Mbps

Command-Line Output

```
add input: udp://239.161.132.1:32000
add output: RTMFP (internal bridge)
NOTE: specified to find first free port between 1935 and 1949
NOTE: testing ports in order: 1947 1942 1946 1943 1940 1938 1937 1941 1945 1944 1949 1935 1939 1936 1948
*** EXTRACTED PORT NUMBER: RTMP 1942
VERSION: 4.master.69 (RELEASE)
Generated Preset:---------------------------
<?xml version="1.0" encoding="UTF-8"?>
<Kulabyte_XML ver="4.2" type="gateway">
   <Input>
```

When the Multicast Agent Diagnostic Tool is opened, 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.

## Location Settings

The following table lists the Location configuration settings:

Information Networking

**Information**

| **Setting** | **Default** | **Description/Values** |
|---|---|---|
| Mgt. Server Location (checkbox) | n/a | Check the checkbox to select this location as the HMP management server. (The auto-generated routes on the gateway assigned to this location will include a loopback destination to HMP.) |
| Name | n/a | Enter a name for the location. This name will be selectable on the Locations list. |
| Default Location | Disabled | Check the checkbox to select this location as the default. The default location's Media Gateway will be used when a user whose IP is not in any of existing location ranges accesses HMP. The default location is displayed in green text in the Locations list. |
| Media Gateways | none | (Optional) Select a gateway that will deliver video to the location from the list of paired Media Gateways (if available). See **Configuring HMP-Media Gateway Pairings**. |

Information Networking

**Networking**

| Setting | Default | Description/Values |
|---|---|---|
| HMP Connection Mode | Rendezvous for regular HMP systems/<br>Listener for HA cluster configurations | (Management Server Location only) The gateway(s) 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:<br>• Rendezvous<br>• Listener<br>• Caller<br>**Note**<br>When HMP is in High Availability (HA) mode, the HMP Connection Mode is "Listener" (read-only).<br>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". |
| Link Connection Mode | Any | Select the link connection mode between locations on your network:<br>• Any<br>• Listener<br>• Caller |
| Outputs | Muxed HLS and Variant HLS enabled | Check as many as apply to configure the recording output(s) generated for each multi-site live source in each location to which they are routed:<br>• Muxed HLS<br>• Variant HLS<br>• SRT<br>**Note**<br>Uncheck the first two boxes to disable either or both of the Muxed HLS (HLS v3) and/or Variant HLS (HLS v4) outputs.<br>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 will then prefer SRT over HLS and be returned a suitable endpoint on the local HMG. |
| Limit | n/a | (Optional) Enter the maximum bandwidth in Mbps to control the rate of outbound traffic to this location. |
| HLS Segment Duration | 10 | (Optional) Enter the 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 will take too long for the playlist to become available and the initial request will be forced to time out. |

| Setting | Default | Description/Values |
|---|---|---|
| SRT Latency (HMP 3.0.1+ only) | 500 | (Optional) Specify the SRT output latency in milliseconds. |
| UDP ToS | 0x88 | (Optional) Enter the desired UDP Type of Service value in hex format (0x00 - 0xFF). |
| IP Address/Mask | n/a | In the first field, type in an IP address for the location. This is a unique IPv4 address in dotted-decimal format (xxx.xxx.xxx.xxx).<br>To specify a subnet mask for the location, type in a netmask in the second field, either in dotted-decimal format (e.g., 255.255.0.0) or CIDR notation.<br>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 / subnet masks for a location. |
| Multicast Address/Mask | n/a | For multicast delivery, specify the multicast address and subnet mask for the location. To disable multicast, leave the Multicast Address empty. |
| Multicast AES+FEC | disabled | ✓ **Tip**<br>Typically you might turn off encryption due to interoperability issues with non-Haivision devices |
| Disable Unicast Fallback | disabled | Check this checkbox to prevent users from falling back to HLS streaming if there are problems with the multicast.<br>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.<br>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. |
| +Network | n/a | Click to add another IP address and subnet mask for the location. |
| +Multicast Range | n/a | Click to specify additional multicast addresses and subnet masks for the location. |

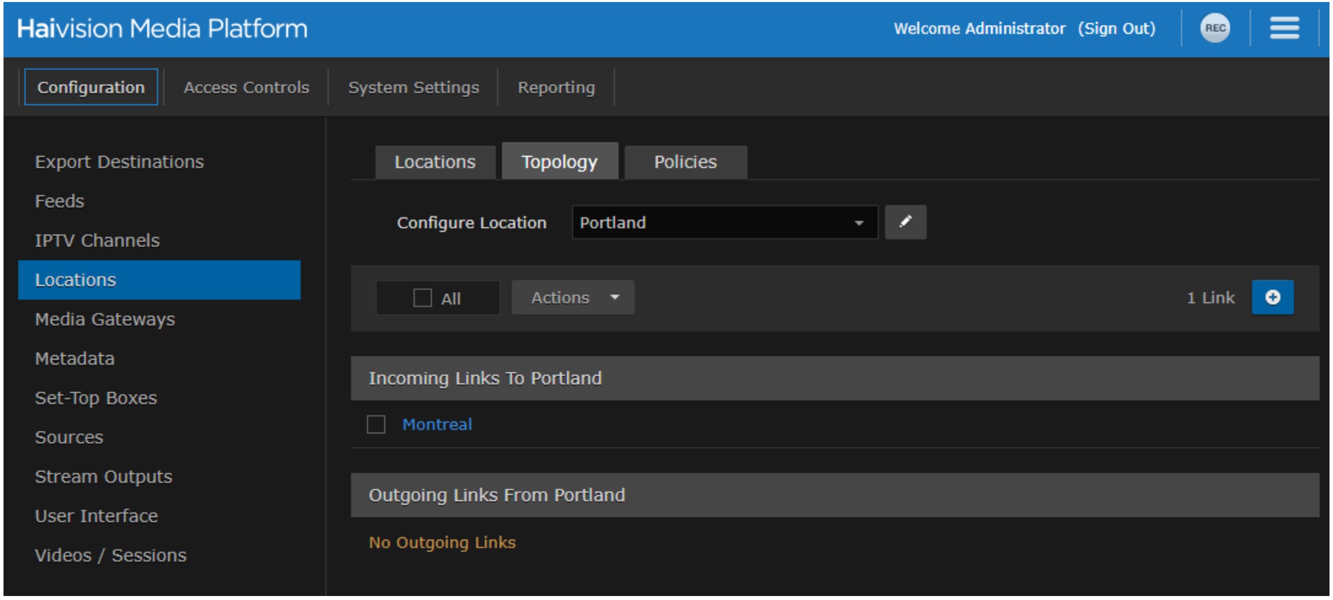
## Locations Topology

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, as well as 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 (see following example). The default location is automatically selected.



Configure Location: Portland

1 Link

Incoming Links To Portland

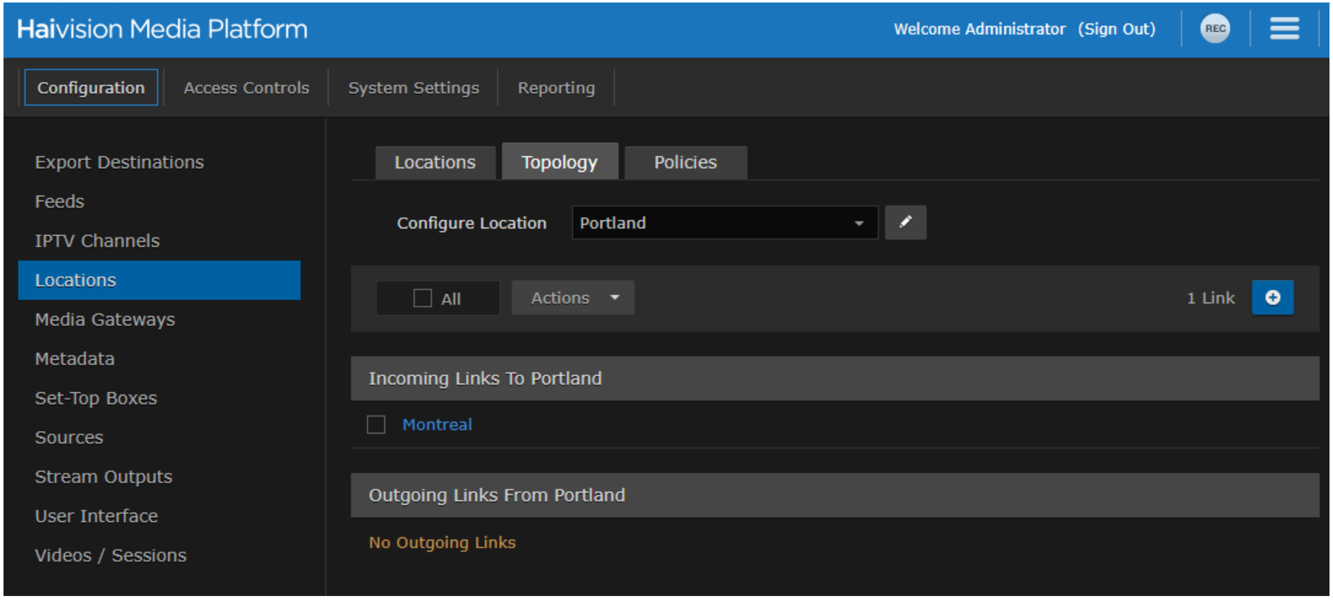
□ Montreal

Outgoing Links From Portland

No Outgoing Links

2. 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.
3. 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 will switch to Portland for the Location and show the defined links, in this example, an Incoming link from Montreal, but no

Outgoing links.



Configure Location: Portland

□ All

Incoming Links To Portland

□ Montreal

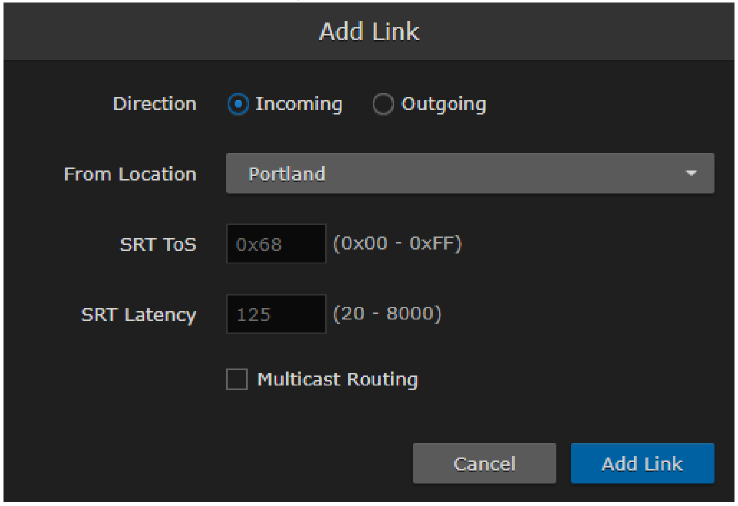
Outgoing Links From Portland

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.



Add Link

Direction: ● Incoming ○ Outgoing

From Location: Portland

SRT ToS: 0x68 (0x00 - 0xFF)

SRT Latency: 125 (20 - 8000)

□ Multicast Routing

3. **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 will default to the sending location's ToS value.

4. **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**.

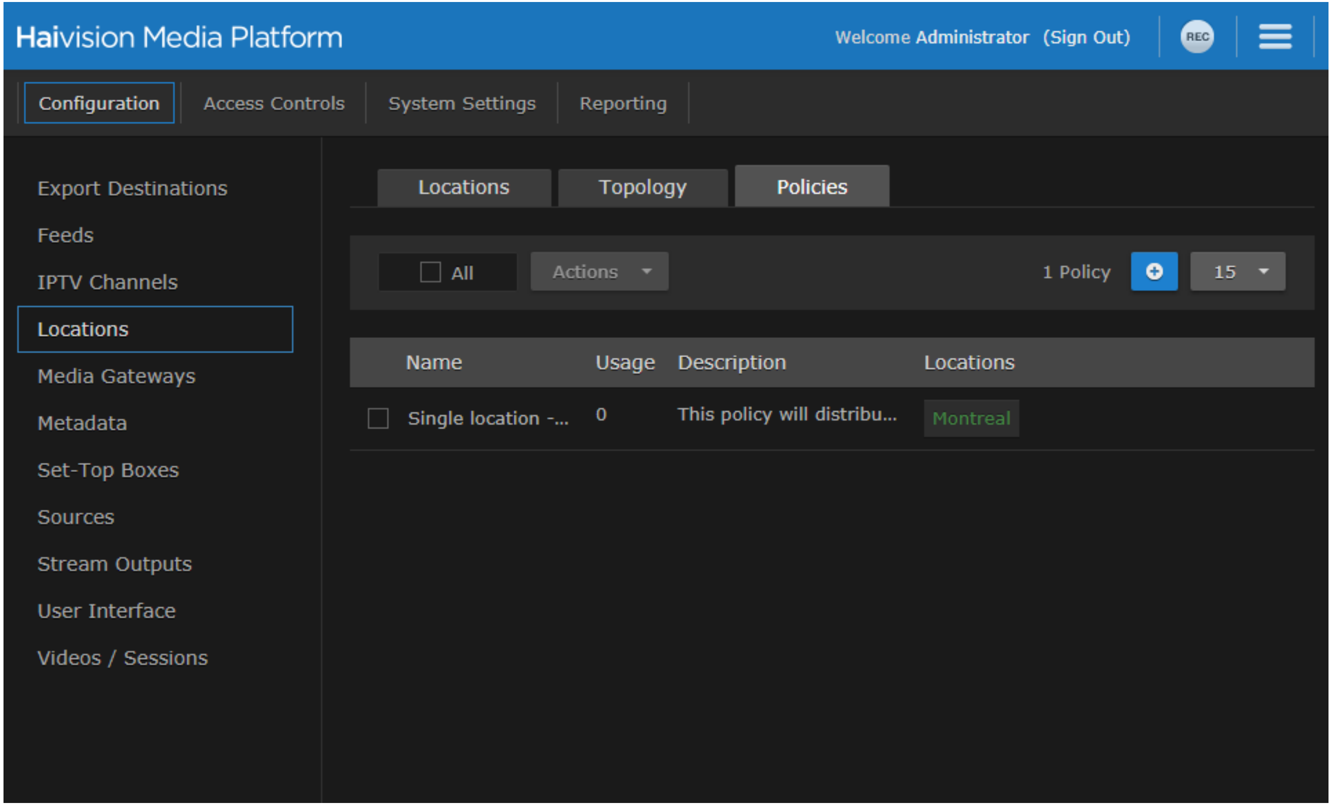
## Locations Policies

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 will be 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.

> **Note**
>
> For systems upgraded to Version 2.6, all existing sessions will follow the existing Location Topology (i.e., all sessions and events are distributed to all locations).

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).

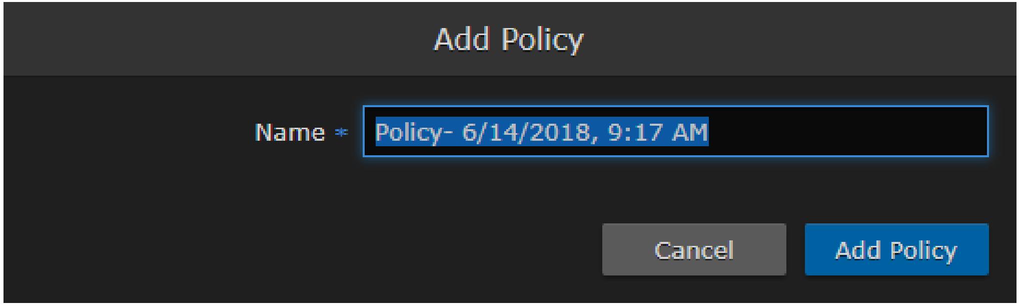


| | Name | Usage | Description | Locations |
|---|---|---|---|---|
| □ | Single location -... | 0 | This policy will distribu... | Montreal |

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.



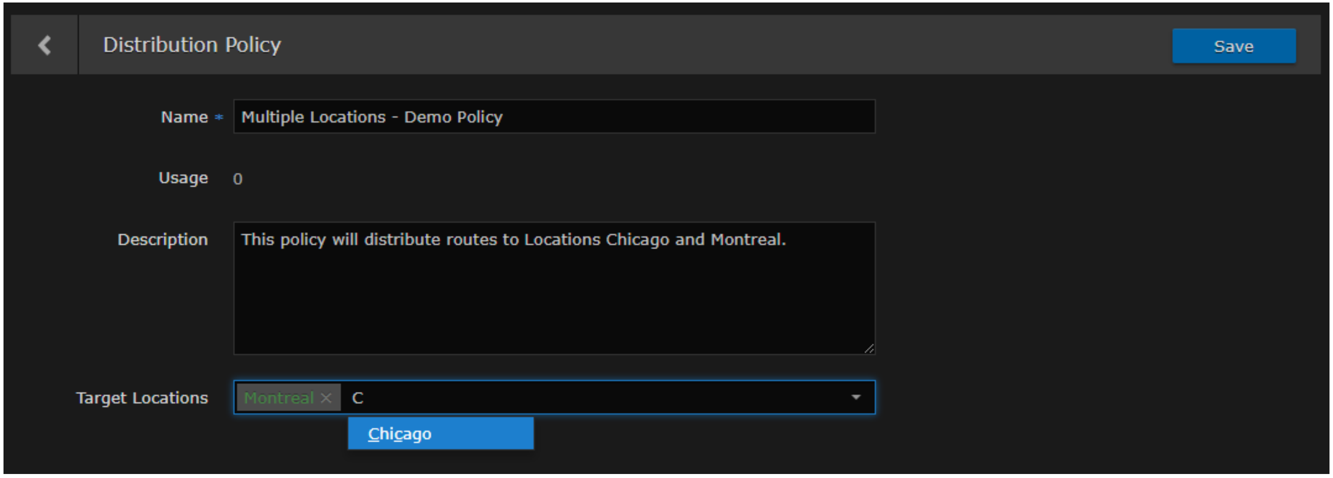
Add Policy

Name * Policy- 6/14/2018, 9:17 AM

3. Click **Add Policy**.
4.

> **Tip**
>
> It's a good idea to provide a clear description of each policy to guide Content Creators as to which policy to use for different scenarios.

5. 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.



Distribution Policy

Name * Multiple Locations - Demo Policy

Usage 0

Description This policy will distribute routes to Locations Chicago and Montreal.

Target Locations Montreal × C

The policy is then added to the list.

6. To configure multiple policies, repeat Step 1 through Step 5.
   These policies are now available in the Sessions/Events Information pane for Content Creators to select.

## Configuring HMP-Media Gateway Pairings

During setup, administrators can pair HMP with one or more Haivision Media Gateways in order 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 will watch video from their local gateway device (although they will 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.

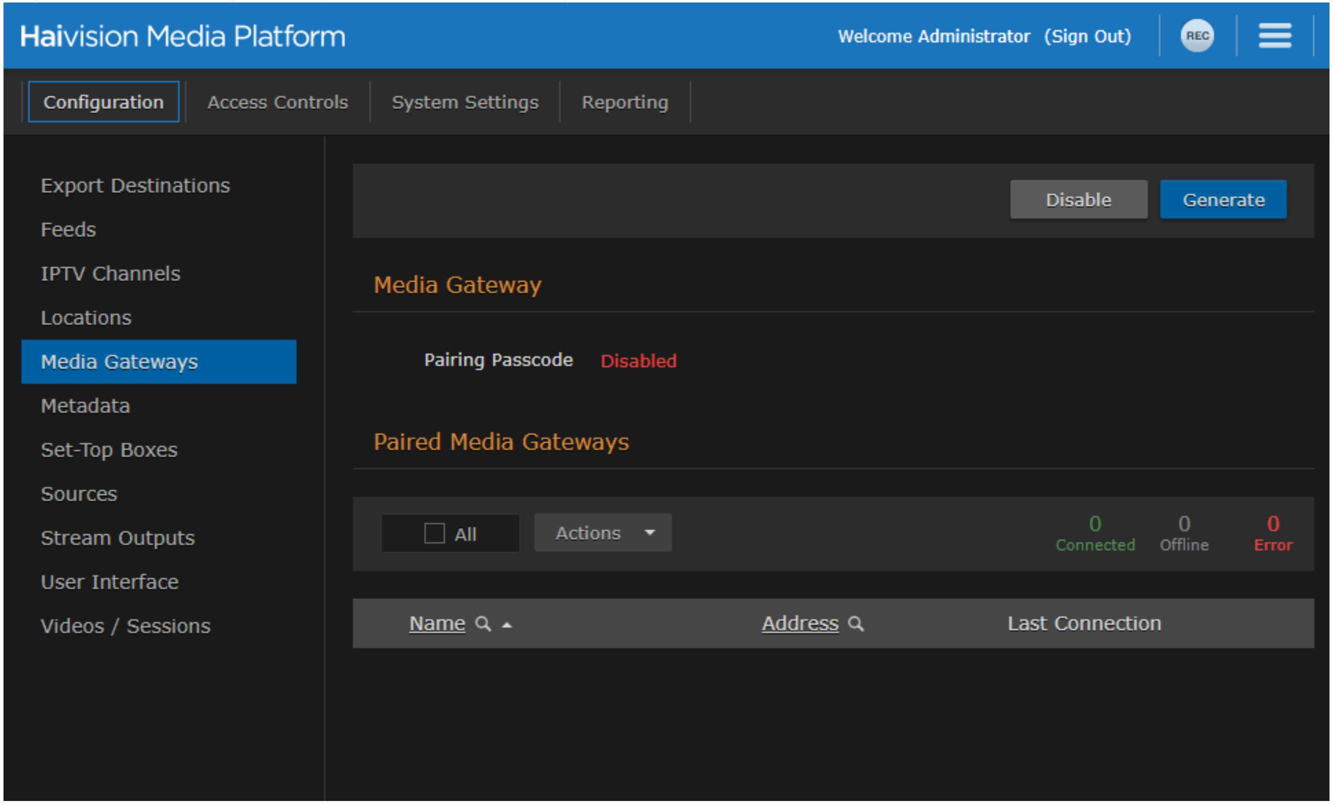
**Topics Discussed**

- Configuring Paired Media Gateways
- Configuring Multi-Site Live Distribution

## Configuring Paired Media Gateways

To view and manage gateway pairings:

1. On the Administration screen, 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**

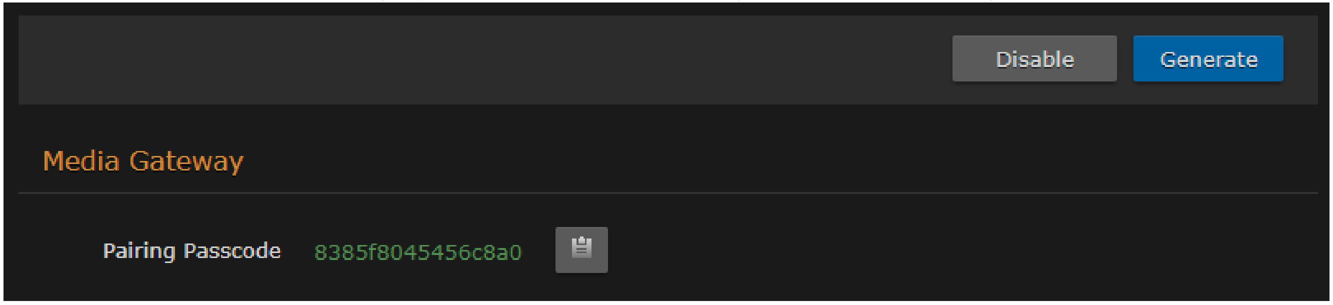
Media Gateway devices initiate outbound requests to HMP to avoid issues with firewall transversal. By default, the HMP Pairing Passcode is “Disabled” as a security measure, meaning that HMP is not accepting any pairing requests.

To add a gateway pairing:

**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.

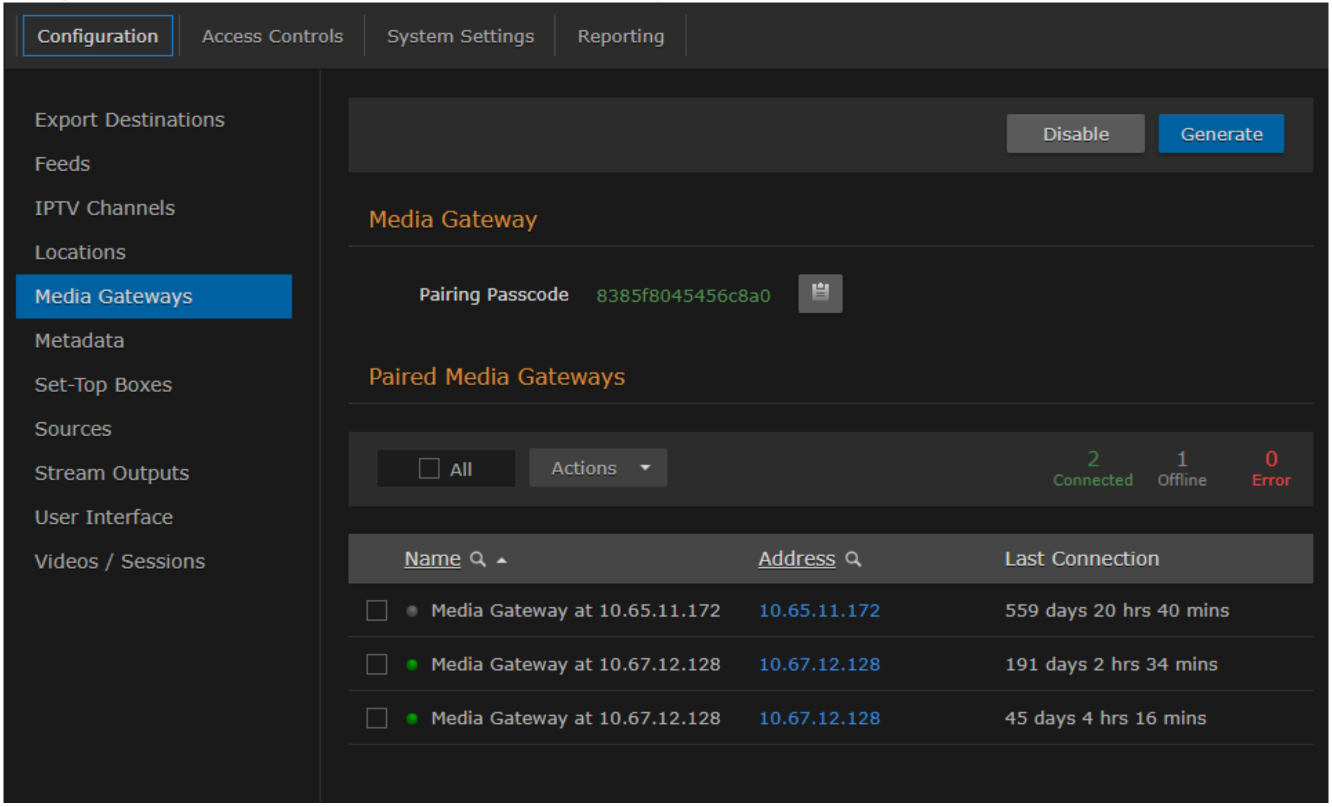
1. On the (HMP) Media Gateways pane, click **Generate** to generate the Pairing passcode.



Media Gateway

Pairing Passcode 8385f8045456c8a0

2. Copy the passcode to the clipboard. (Do not disable yet.)
3. Make note of the HMP address and ports. If there is a cross-domain address, make a note of it as well.
4. On the (Media Gateway) Administration page, click **Configuration** on the toolbar and then click Media Gateways **Media Platform** on the sidebar. In the Gateway section of the Settings pane, enter the Media Gateway information as needed.
5. 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. Click **Pair**. For details, refer to the Media Gateway User's Guide.
   On the (Media Gateway) Media Platform configuration pane, define the Gateway and HMP settings and paste the Pairing passcode into the Passcode field. For details, refer to the Media Gateway User's Guide.
6. On the (HMP) 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.



Media Gateway

Pairing Passcode 8385f8045456c8a0

Paired Media Gateways

2 Connected 1 Offline 0 Error

| | Name | Address | Last Connection |
|---|---|---|---|
| □ | ● Media Gateway at 10.65.11.172 | 10.65.11.172 | 559 days 20 hrs 40 mins |
| □ | ● Media Gateway at 10.67.12.128 | 10.67.12.128 | 191 days 2 hrs 34 mins |
| □ | ● Media Gateway at 10.67.12.128 | 10.67.12.128 | 45 days 4 hrs 16 mins |

**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 tab.

7. On the (HMP) Administration page, click **Locations** on the sidebar.
On the (HMP) Locations Information pane, this gateway is now available for selection from the list of paired Media Gateways. (See Step #5 on Managing Locations.)
8. On the (HMP) Media Gateways pane, click **Disable** to block any new connections.

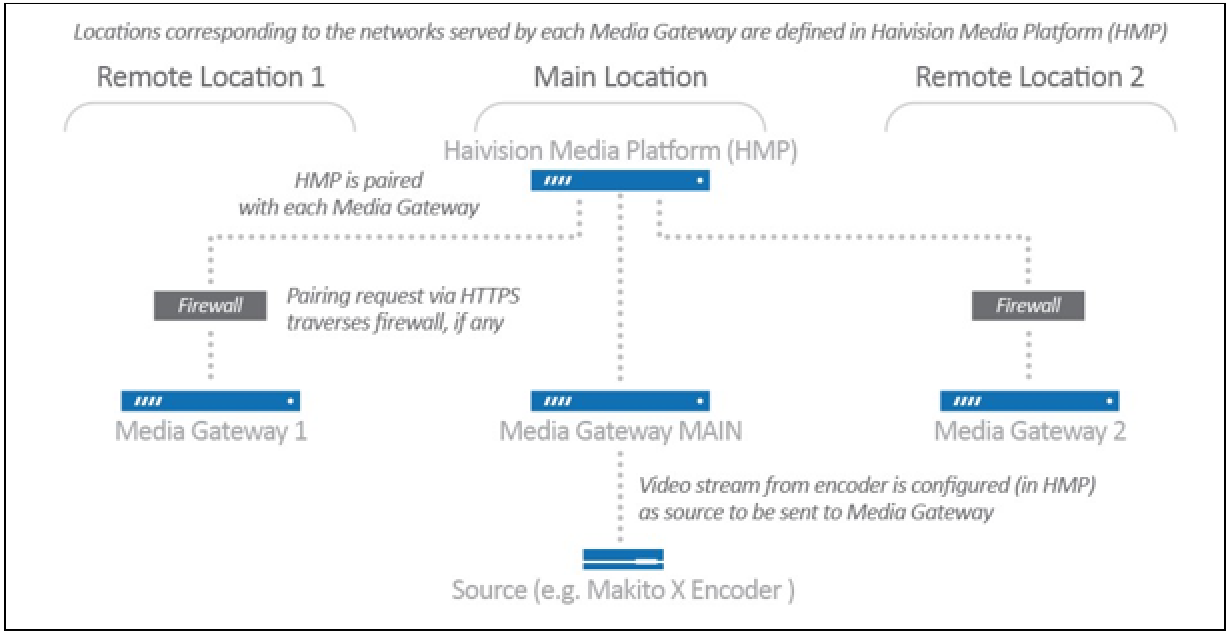
## Configuring Multi-Site Live Distribution

**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.

**To configure multi-site live distribution:**

1. Pair one or more Media Gateways with your HMP, following steps in Configuring Paired Media Gateways. Any paired gateways will be listed on the (HMP) Media Gateways list.

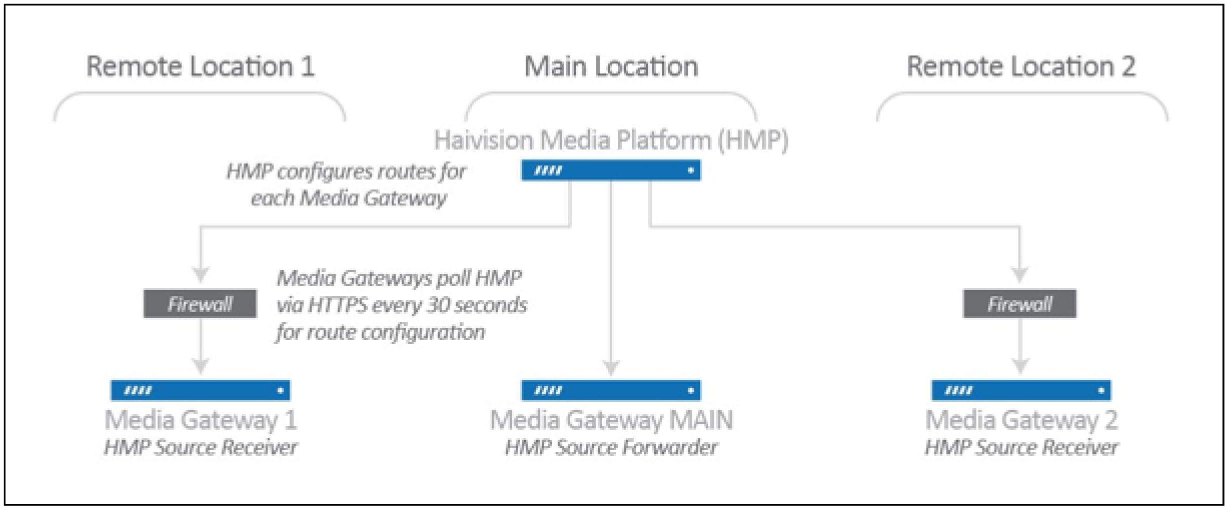

Locations corresponding to the networks served by each Media Gateway are defined in Haivision Media Platform (HMP)
Remote Location 1
Main Location
Remote Location 2
Haivision Media Platform (HMP)
HMP is paired with each Media Gateway
Firewall
Pairing request via HTTPS traverses firewall, if any
Firewall
Media Gateway 1
Media Gateway MAIN
Media Gateway 2
Video stream from encoder is configured (in HMP) as source to be sent to Media Gateway
Source (e.g. Makito X Encoder )

**Tip**

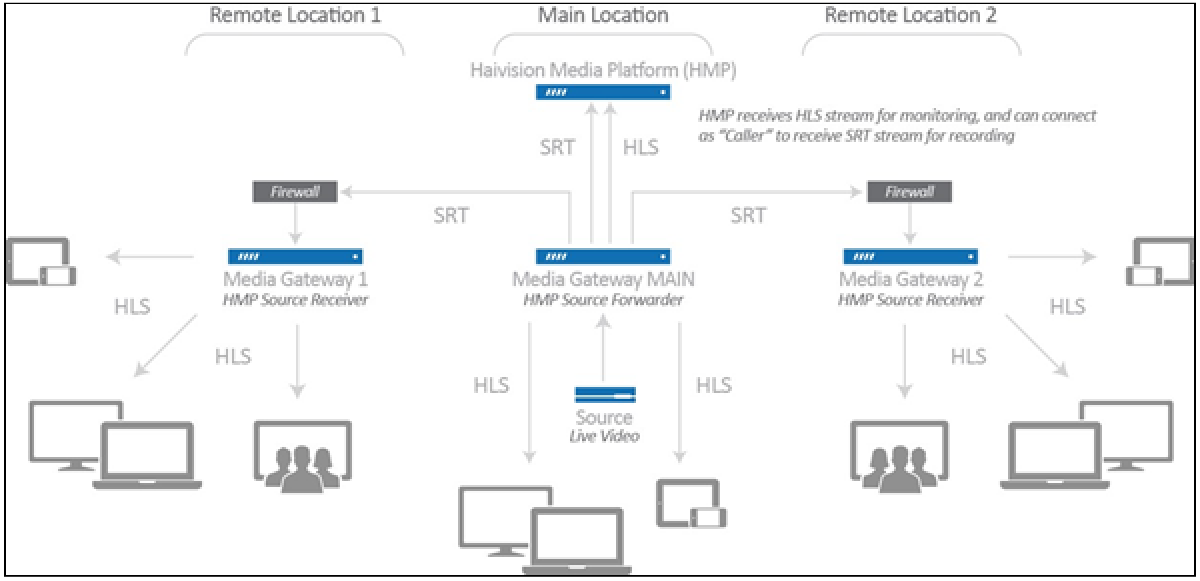
You can use the same pairing passcode while pairing multiple gateways. We recommend that you disable the passcode after all gateways have been connected. It can always be turned back on to add a new gateway to the network.

2. 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.
3. On the (HMP) Locations list, select the Mgt. Server Location, i.e., the location of the HMP management server. For example, referring to the previous diagram, Media Gateway “MAIN” is selected as the Management Server Location since this gateway and HMP are at the same location

i.e., Main Location.



4. On HMP, create one or more Sources, selecting one of the paired Media Gateways for the Receiver. For details, see **Configuring Sources**. For example, referring to the following diagram, while creating a source with “MXE Source,” Media Gateway “MAIN” should be selected as the receiver.
5. Create a Session with one of the configured Sources. Based either on the Schedule or “Live” state, multi-site routes will automatically be created on all paired Media Gateways.



Live multi-site routes will be created on all paired Media Gateways when a source belongs to an active Session. Specifically, multi-site Gateway routes will be 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 will have active multi-site routes regardless of its “Live” state. All configured gateways will 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.**

# Configuring 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 Content 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**

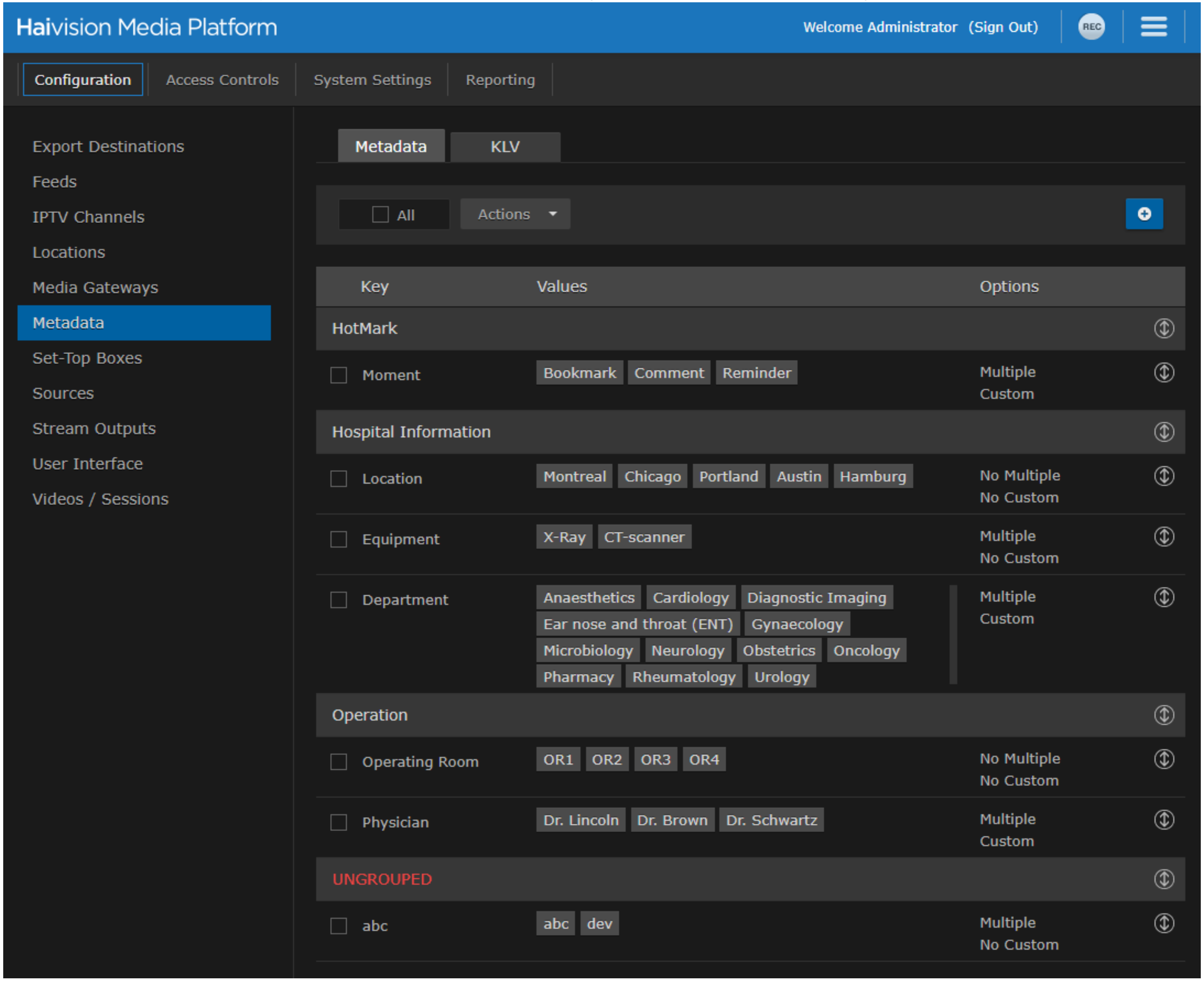
Viewers only see metadata assigned to videos for which they have access

**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. (Note that metadata cannot be sorted on mobile devices because they do not have the same drag and drop support as desktop Web browsers.)**

To view and configure metadata:

1. On the Administration screen, 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.

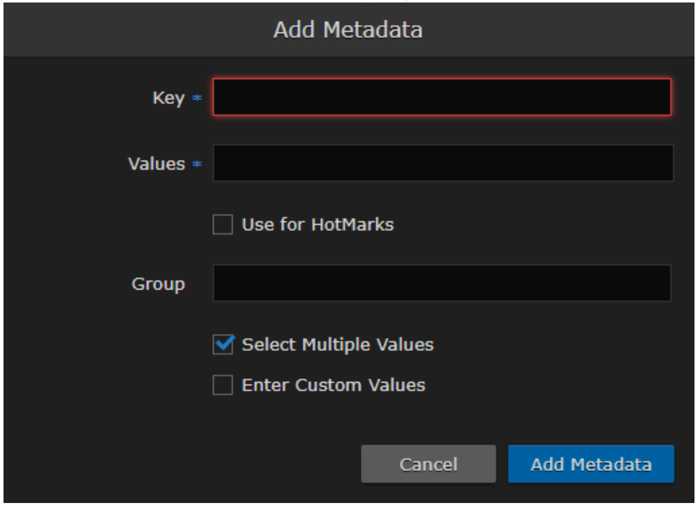


| Key | Values | Options |
|---|---|---|
| HotMark | | |
| □ Moment | Bookmark Comment Reminder | Multiple<br>Custom |
| Hospital Information | | |
| □ Location | Montreal Chicago Portland Austin Hamburg | No Multiple<br>No Custom |
| □ Equipment | X-Ray CT-scanner | Multiple<br>No Custom |
| □ Department | Anaesthetics Cardiology Diagnostic Imaging Ear nose and throat (ENT) Gynaecology Microbiology Neurology Obstetrics Oncology Pharmacy Rheumatology Urology | Multiple<br>Custom |
| Operation | | |
| □ Operating Room | OR1 OR2 OR3 OR4 | No Multiple<br>No Custom |
| □ Physician | Dr. Lincoln Dr. Brown Dr. Schwartz | Multiple<br>Custom |
| UNGROUPED | | |
| □ abc | abc dev | Multiple<br>No Custom |

To define metadata:

1. On the Metadata pane, click the ⊕ icon.

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



Add Metadata

Key *

Values *

□ Use for HotMarks

Group

☑ Select Multiple Values

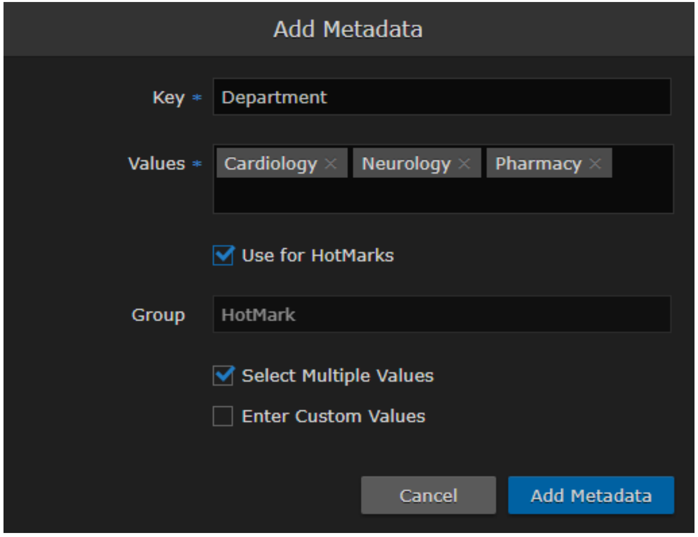
□ Enter Custom Values

3.

> **Note**
>
> By default, users will be 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 ✖ icon.

4. To use the Metadata for HotMarks, check the checkbox. Note that “HotMarks” will serve as the group for the metadata.



Add Metadata

Key * Department

Values * Cardiology × Neurology × Pharmacy ×

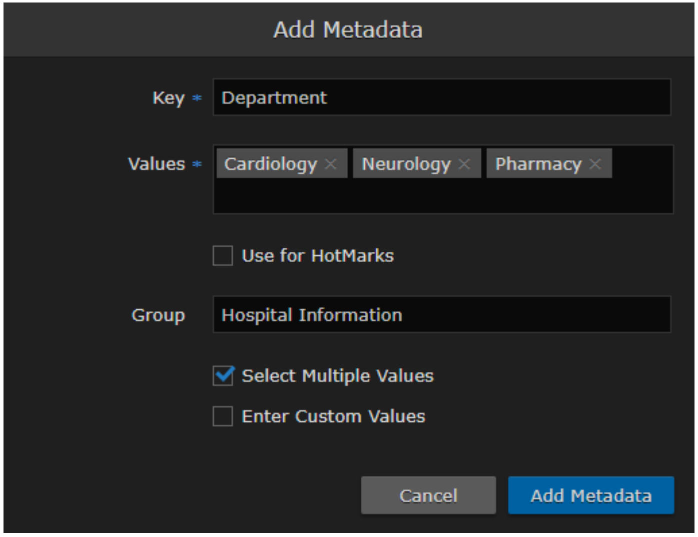
☑ Use for HotMarks

Group HotMark

☑ Select Multiple Values

□ Enter Custom Values

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



Add Metadata

Key * Department

Values * Cardiology × Neurology × Pharmacy ×

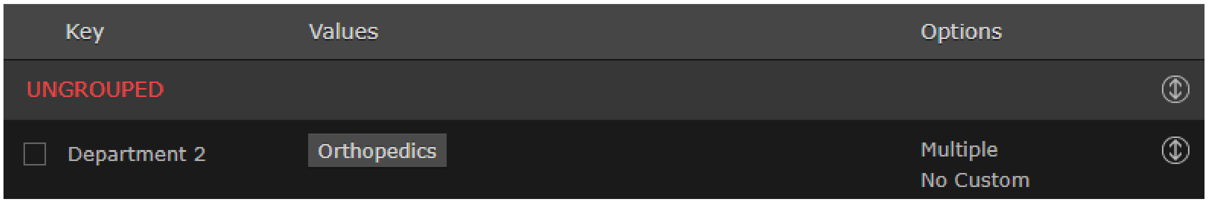
☐ Use for HotMarks

Group Hospital Information

☑ Select Multiple Values

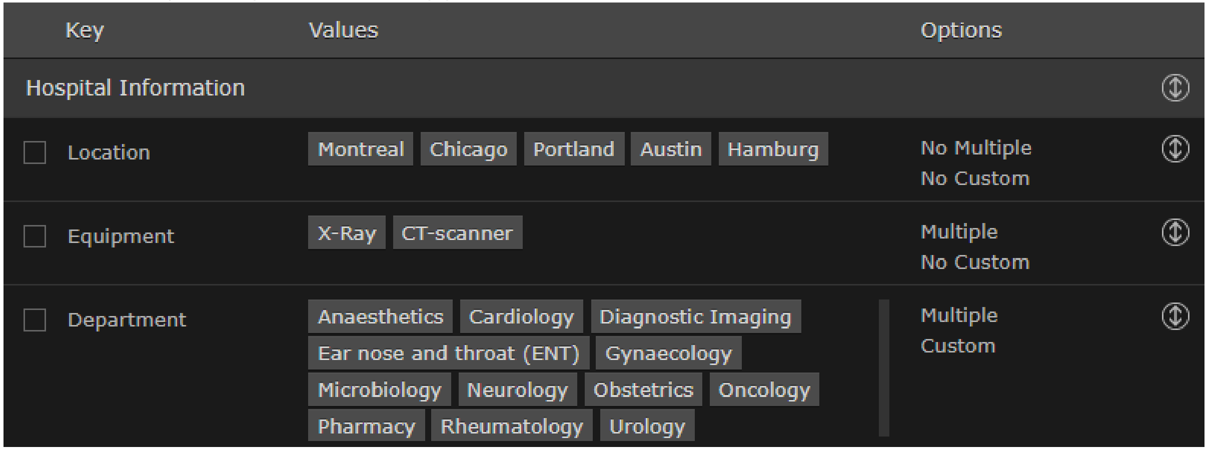
☐ Enter Custom Values

> **Tip**
>
> If you do not assign a group to the metadata or select it for use with HotMarks, it will be listed as “UNGROUPED”.



| Key | Values | Options |
|---|---|---|
| UNGROUPED | | |
| ☐ Department 2 | Orthopedics | Multiple<br>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 will be 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 | | |
| ☐ Location | Montreal Chicago Portland Austin Hamburg | No Multiple<br>No Custom |
| ☐ Equipment | X-Ray CT-scanner | Multiple<br>No Custom |
| ☐ Department | Anaesthetics Cardiology Diagnostic Imaging Ear nose and throat (ENT) Gynaecology Microbiology Neurology Obstetrics Oncology Pharmacy Rheumatology Urology | Multiple<br>Custom |

**Tip**

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

**Important**

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

For details, see Managing KLV Inputs.

**Topics Discussed**

- Metadata Settings
- Managing KLV Inputs

## Metadata Settings

The following table lists the Metadata configuration settings:

| Metadata Setting | Default | Description/Values |
|---|---|---|
| Key | n/a | The label for the metadata. |
| Values | n/a | One or more default values that can be selected by users for this metadata. |
| Use for HotMarks | Disabled | Check this checkbox to add this metadata to the HotMarks list instead of the general Metadata list. |
| Group | n/a | (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 | Check this checkbox to allow users to add more than one value to this metadata key. |
| Enter Custom Values | Disabled | Check this checkbox to allow 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.

**Haivision Media Platform supports KLV data parsing and display as a licensable option per system. Administrators can create and upload a metadata dictionary file to customize and dynamically display KLV metadata to provide context with associated video/audio streams.**

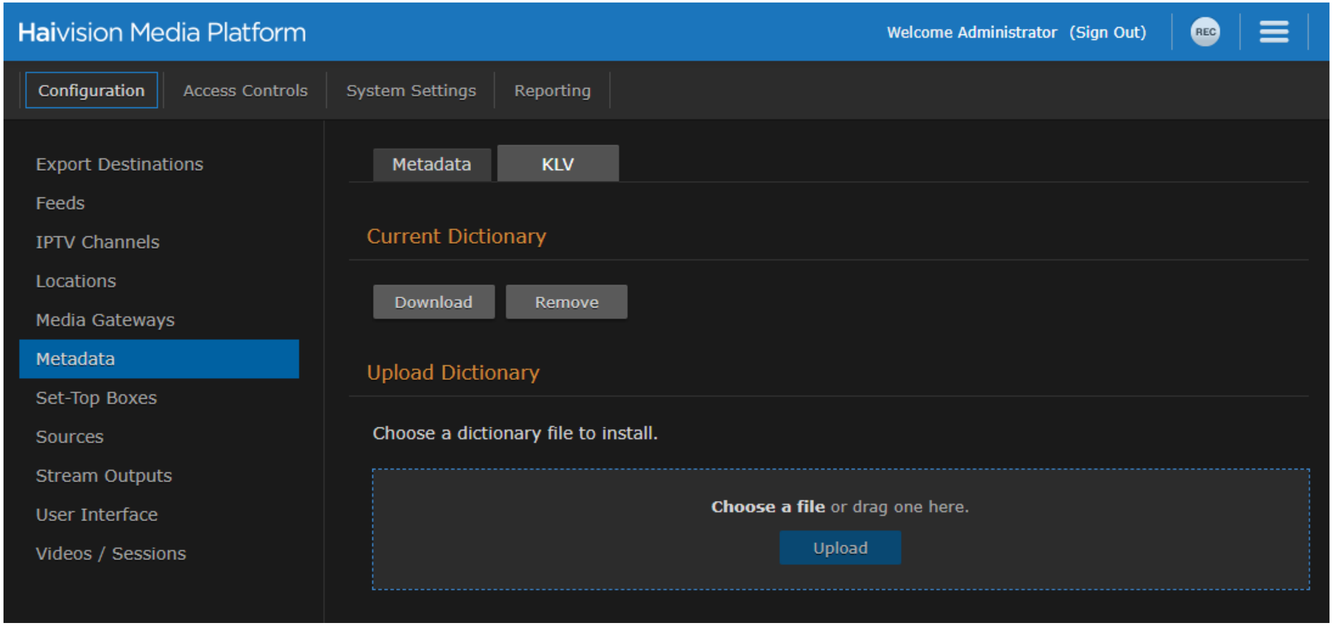
To accommodate changes to the KLV dictionary, HMP accepts a library file which will translate the KLV data being sent into human readable fields and units of measure. The library file is in JSON format and complies with MISB RP 0602.2 and Standard 0604.1.

Administrators can also download and review the currently uploaded KLV dictionary.

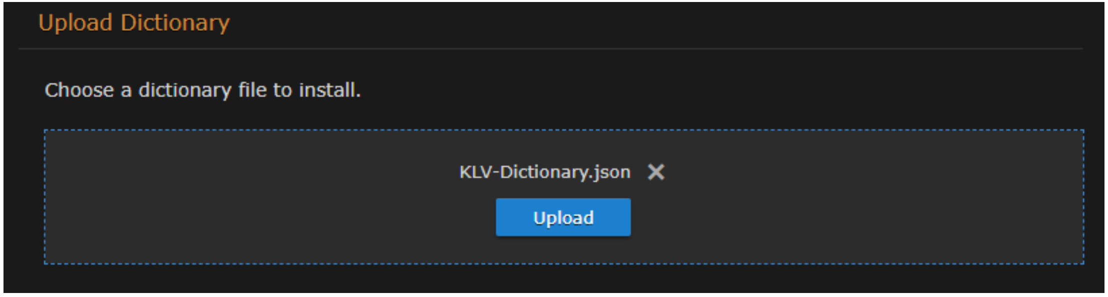
On the Content Library screen, users can turn on/off the display of KLV data in a sidebar in the multi-window viewer.

To manage KLV inputs:

1. On the Metadata pane, click the **KLV** tab.
   The KLV pane opens (as shown in the following example).



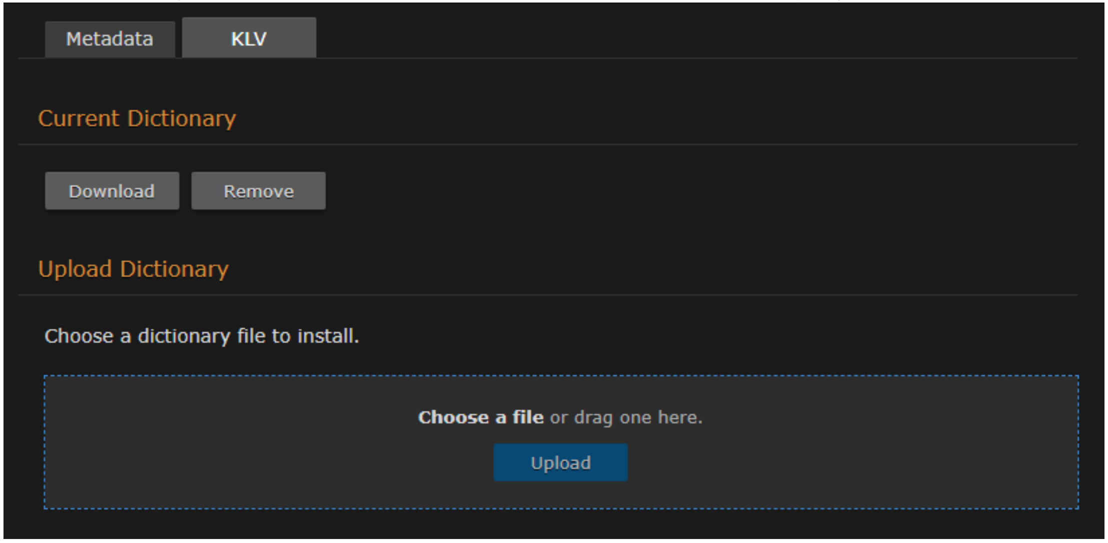
2. To upload a dictionary, drag a file to the drop area or click **Choose a file** and select the dictionary file to load. For details on the dictionary file format, see KLV Dictionary Format.
   A sample dictionary file is available on Haivision's Support Portal at: https://support.haivision.com
3. When you see the filename in the drag area, click **Upload**.



**Tip**

To select a different dictionary file, click Change. To remove the selection, click the ✕ icon.

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



Metadata
KLV
Current Dictionary
Download
Remove
Upload Dictionary
Choose a dictionary file to install.
Choose a file or drag one here.
Upload

4. To view the currently installed dictionary, click **Download**. You can then open the file in a text editor to view the KLV dictionary.
5. To remove the currently installed dictionary from your system, click **Remove**.

# STB Administration

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 tagbased configuration of devices.

When a new set-top box is registered 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 boots up.

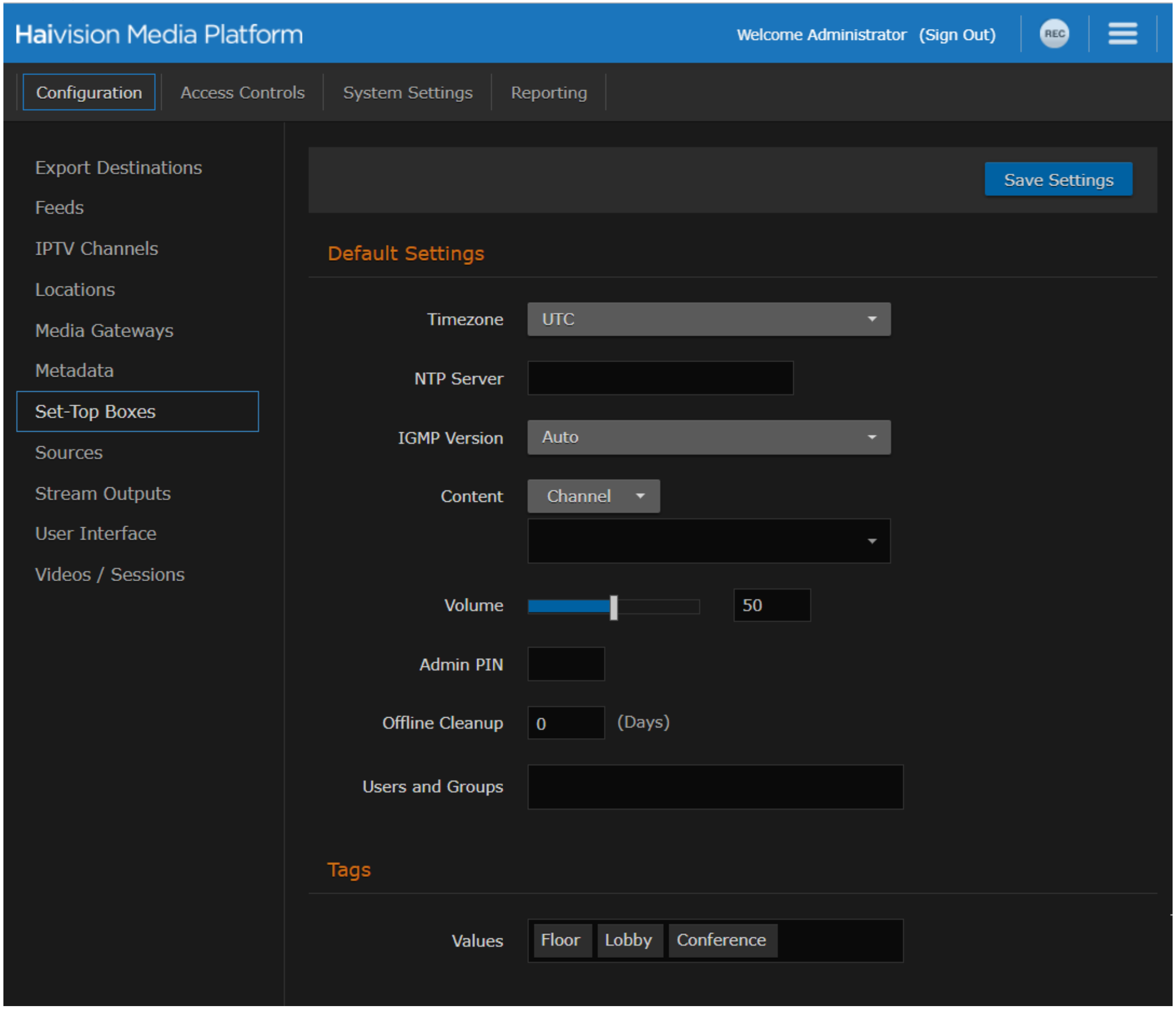
**Topics Discussed**

- Setting Device Defaults
- Tagging Devices

## Setting Device Defaults

To configure default device settings:

1. On the Administration screen, 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).



Default Settings

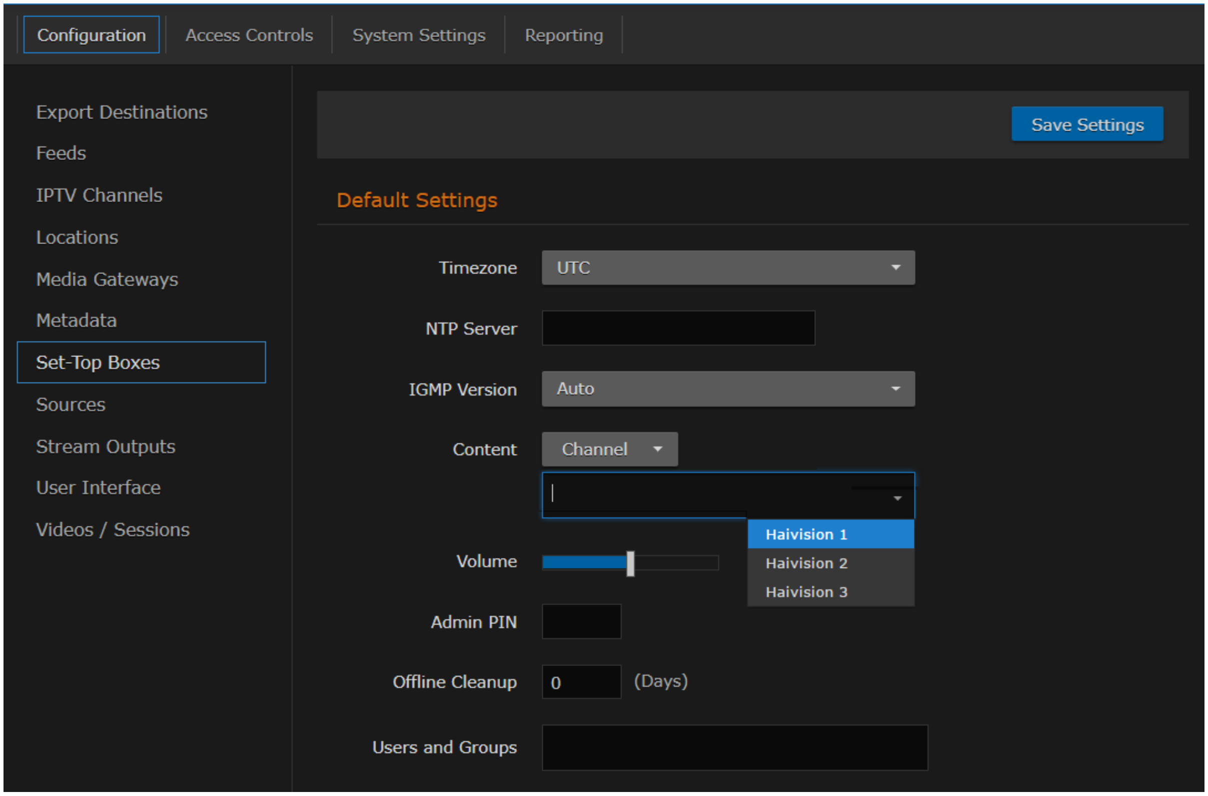
Timezone: UTC
NTP Server:
IGMP Version: Auto
Content: Channel
Volume: 50
Admin PIN:
Offline Cleanup: 0 (Days)
Users and Groups:

Tags

Values: Floor Lobby Conference

2. Enter or select the value(s) to serve as default device settings. See **Device Default Settings**.
   The changes take effect immediately and will apply to new STBs registered with the server.

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



Timezone: UTC

NTP Server:

IGMP Version: Auto

Content: Channel

Volume

Admin PIN:

Offline Cleanup: 0 (Days)

Users and Groups:

4. Click **Save Settings**.

### Related Topics

- Device Default Settings

## Device Default Settings

The following table lists the Device Default settings:

Default Settings Device Tags

### Default Settings

| Setting | Description/Values |
|---|---|
| Timezone | **Note**<br>The times are based on hours added to or subtracted from Greenwich Mean Time (GMT). |
| NTP Server | This is blank the first time you open the (HMP) Manage Devices screen after an upgrade. Once the default is set, it is applied to new STBs registered.<br>**Note**<br>Haivision Play 1000 STBs do not support FQDNs for the NTP server. Use an IP address only.<br>**Tip**<br>Generally, it is recommended to use the same NTP server as HMP. |
| IGMP Version | Initially set to Auto. If required by your system, select IGPMv2 or IGMPv3. |
| Content | Select the default content type for the device, either Channel, Videos, or Session. Then select the channel, video, or session title from the drop-down list. |
| 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 | (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.<br>**Tip**<br>If you are not using an Admin PIN, clear the input field (leave it empty) and click **Save**. |
| Offline Cleanup | To set the offline cleanup period, enter the number of days. Devices offline for more than the specified cleanup period will be removed from the Devices list.<br>To disable automatic cleanup, set to 0 (default). |
| Users and Groups | Type in the name(s) of defined users and groups to assign access to the STB content. |

Default Settings Device Tags

### Device Tags

| Setting | Description/Values |
|---|---|
| Values | Type in one or more words or phrases to describe and manage the device. See Tagging Devices. |

## Tagging Devices

Tag-based configuration facilitates online management of large installations of devices. 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.

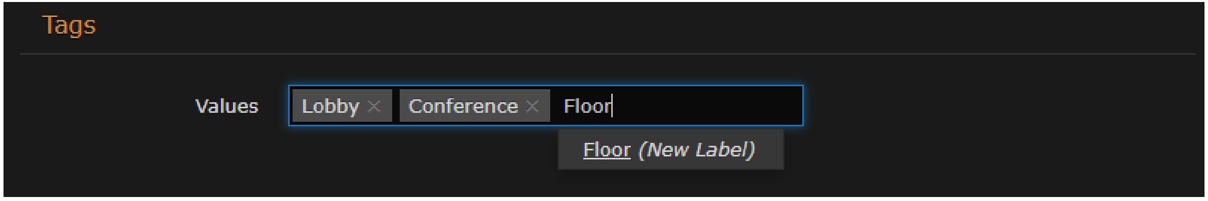
Tags are similar to, but more specific than groups and are generally used to describe and manage devices with more granularity.

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.

Once devices are tagged, you can filter by tags to view, edit or schedule only devices that share selected tags. This is useful to narrow down 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. On the Set-Top Boxes pane, scroll to the bottom to view the defined tags for the HMP domain.
2. To add a new tag, click in the **Tags** text box, type in the tag name, and press **Enter**.



Tags

Values: Lobby ×, Conference ×, Floor

3. 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 as well as share the source with other users or groups.

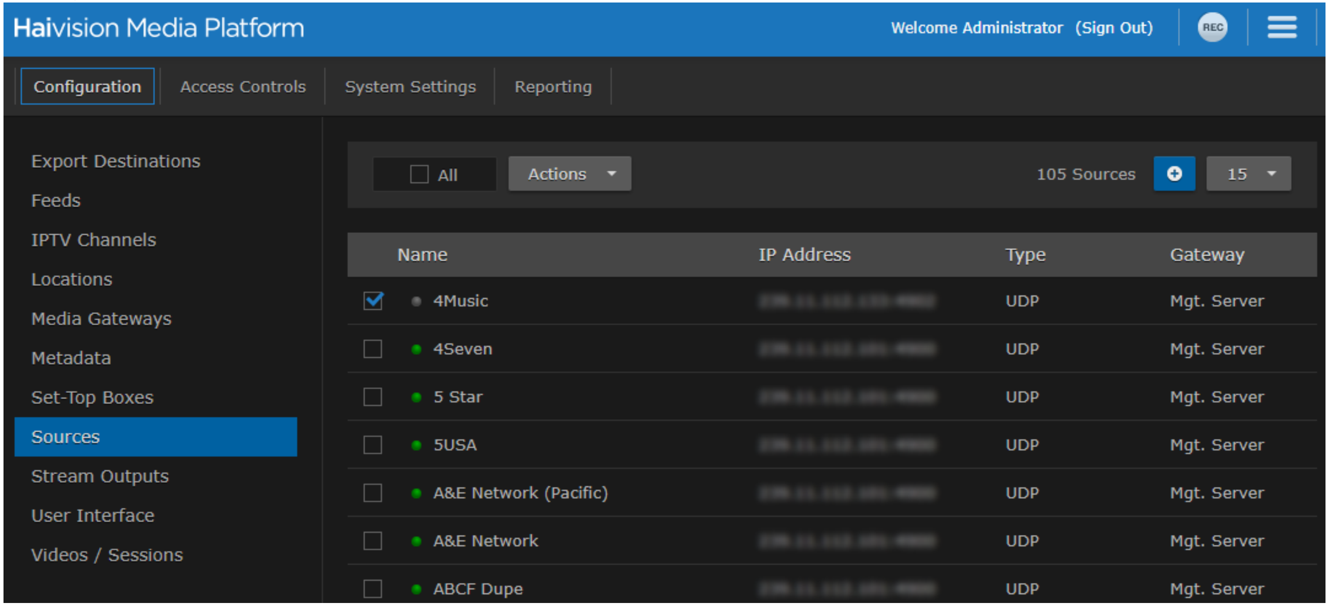
The protocol types are UDP or SRT (Haivision's Secure Reliable Transport) streaming protocol. With UDP, you can select multicast or unicast streaming. SRT optimizes streaming performance across unpredictable networks, including the public Internet.

**Note**

Users can view source content before creating a session on the Content Library screen. See **Previewing Sources** (in the**User's Guide**).

**To view and manage sources:**

1. On the Administration screen, 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).



| | Name | IP Address | Type | Gateway |
|---|---|---|---|---|
| ☑ | 4Music | [redacted] | UDP | Mgt. Server |
| □ | 4Seven | [redacted] | UDP | Mgt. Server |
| □ | 5 Star | [redacted] | UDP | Mgt. Server |
| □ | 5USA | [redacted] | UDP | Mgt. Server |
| □ | A&E Network (Pacific) | [redacted] | UDP | Mgt. Server |
| □ | A&E Network | [redacted] | UDP | Mgt. Server |
| □ | ABCF Dupe | [redacted] | UDP | Mgt. Server |

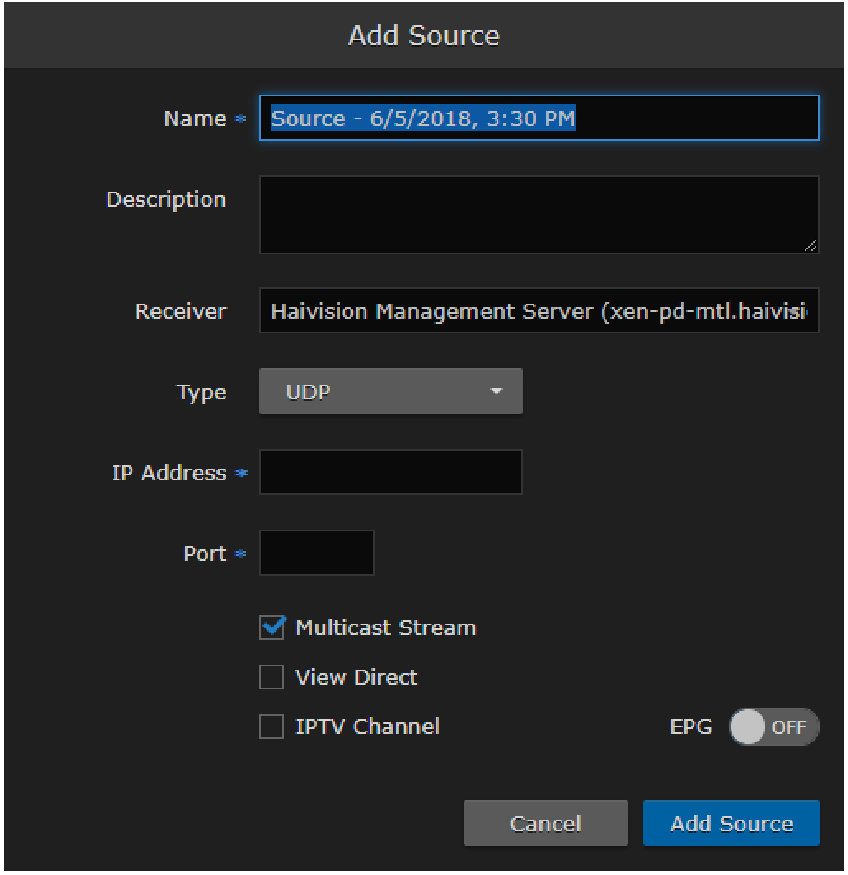
### Topics Discussed

- Configuring Sources
- Source Settings
- Configuring Secure Reliable Transport (SRT) Sources
- SRT Source Statistics

## Configuring Sources

To add a source:

1. From the Sources list (Administration screen), click the ⊕ icon.
2. On the Add Source dialog, type in a name and enter or select the value(s) to define the source. See Source Settings.



Add Source

Name * Source - 6/5/2018, 3:30 PM

Description

Receiver Haivision Management Server (xen-pd-mtl.haivisi

Type UDP

IP Address *

Port *

☑ Multicast Stream

□ View Direct

□ IPTV Channel

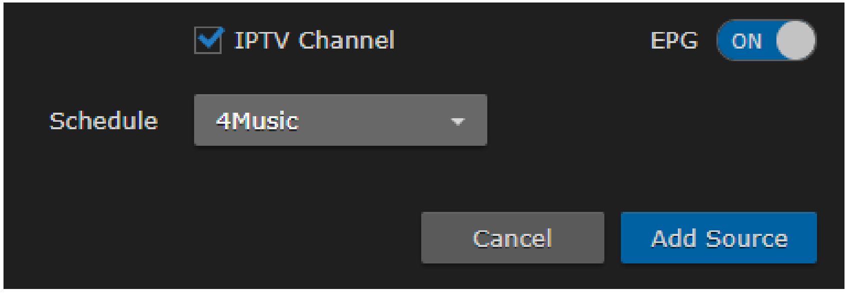
EPG OFF

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 Configuring HMP-Media Gateway Pairings).
  - Media Gateway also allows you to select RTMP or RTSP sources. For details of these settings, see "RTMP Settings" and "RTMP Settings" in Source Settings.

3. To enable the source for IPTV deployment, check the IPTV Channel checkbox.

4. 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.)



☑ IPTV Channel

EPG: ON

Schedule: 4Music

5. Click **Add Source**.
   The new source will be added to the Sources list.

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. Click **Save**.
4. To assign metadata to the source(s), click the **Metadata** tab.
   Metadata keys and values must be pre-defined on your system. See Configuring Metadata.
5. > **Note**
   >
   > If you select multiple sources and the metadata has “mixed” (i.e., different) values, you will see a warning across the top of the list and the metadata with mixed values will be displayed in yellow. For the steps to bulk-edit metadata, see Editing Information and Metadata (in the User's Guide).

6. Click **Save**.
7. To share sources, click the **Share** tab and follow the steps in Sharing Items (in the User's Guide).

## Source Settings

The following table lists the Source configuration settings:

Information SRT Settings RTMP Settings RTSP Settings Metadata

### Information

| Setting | Default | Description/Values |
|---|---|---|
| ID | n/a | **Note**<br>If you are using the HMP Command Line API, you will need to copy this ID to add this source to a session. |
| Name | date, time | Enter a name for the source. This name will be selectable on the Sources list when content creators define sessions. |
| Description | n/a | 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, either:<br>• UDP<br>• SRT (see the SRT Settings section of this table)<br>• RTMP (see the RTMP Settings section of this table)<br>**Note**<br>Available only in multi-site live configurations when Media Gateway is selected in the Receiver dropdown.<br>• RTSP (see the RTSP Settings section of this table)<br>**Note**<br>Available only in multi-site live configurations when Media Gateway is selected in the Receiver dropdown. |
| IP Address | n/a | Type in the IP address for the source. |
| Port | n/a | Type in the port number for the source. |
| Multicast Stream | Enabled | (Type must be UDP) Check this checkbox to indicate this is a multicast stream. |

| Setting | Default | Description/Values |
|---|---|---|
| View Direct | Disabled | (Type must be UDP) Check this checkbox to specify that the Haivision Play Set-Top Box use the configured Source URL directly and not use 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 should still flow through the normal multi-site live distribution mechanism (which requires at least one Media Gateway). |
| IPTV Channel | Disabled | Check this checkbox to specify that the Source should be used in IPTV workflows. It will then be 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 set up IPTV channels and assign access from here or from the IPTV Channels pane. |
| 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

### SRT Source Settings

| Setting | Default | Description/Values |
|---|---|---|
| Mode | Caller | Specifies the SRT Connection Mode:<br>• Caller: HMP acts like a client and connects to a server listening and waiting for an incoming call.<br>• Listener: HMP acts like a server and listens & waits for clients to connect to it.<br>• Rendezvous: Allows calling and listening at the same time.<br>✓ **Tip**<br>To simplify firewall traversal, Rendezvous Mode allows HMP and the encoder to traverse a firewall without the need for IT to open a port.<br>ℹ **Note**<br>See **Configuring Secure Reliable Transport (SRT) Sources**. |
| Latency | 125 ms | Specifies how long HMP will buffer 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).<br>ℹ **Note**<br>Latency is for the SRT protocol only and does not include the capture, encoding, decoding and display processes of the endpoint devices. |
| Passphrase | n/a | (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.<br>Range = 10-79 UTF8 characters |
| Statistics | n/a | Click to view the statistics for the SRT source. See **SRT Source Statistics**. |
| | | |

Information SRT Settings RTMP Settings RTSP Settings Metadata

### RTMP Source Settings

ℹ **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:<br>• 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 *Haivision Media Gateway User's Guide* .<br>• Consumer — Stream available for Media Gateway to access on an RTMP server. |

Information SRT Settings RTMP Settings **RTSP Settings** Metadata

### RTSP Source Settings

> **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**

### Metadata

| Setting | Default | Description/Values |
|---|---|---|
| Metadata | n/a | **Note**<br>Metadata keys and values must be pre-defined on your system. See **Configuring Metadata**. |

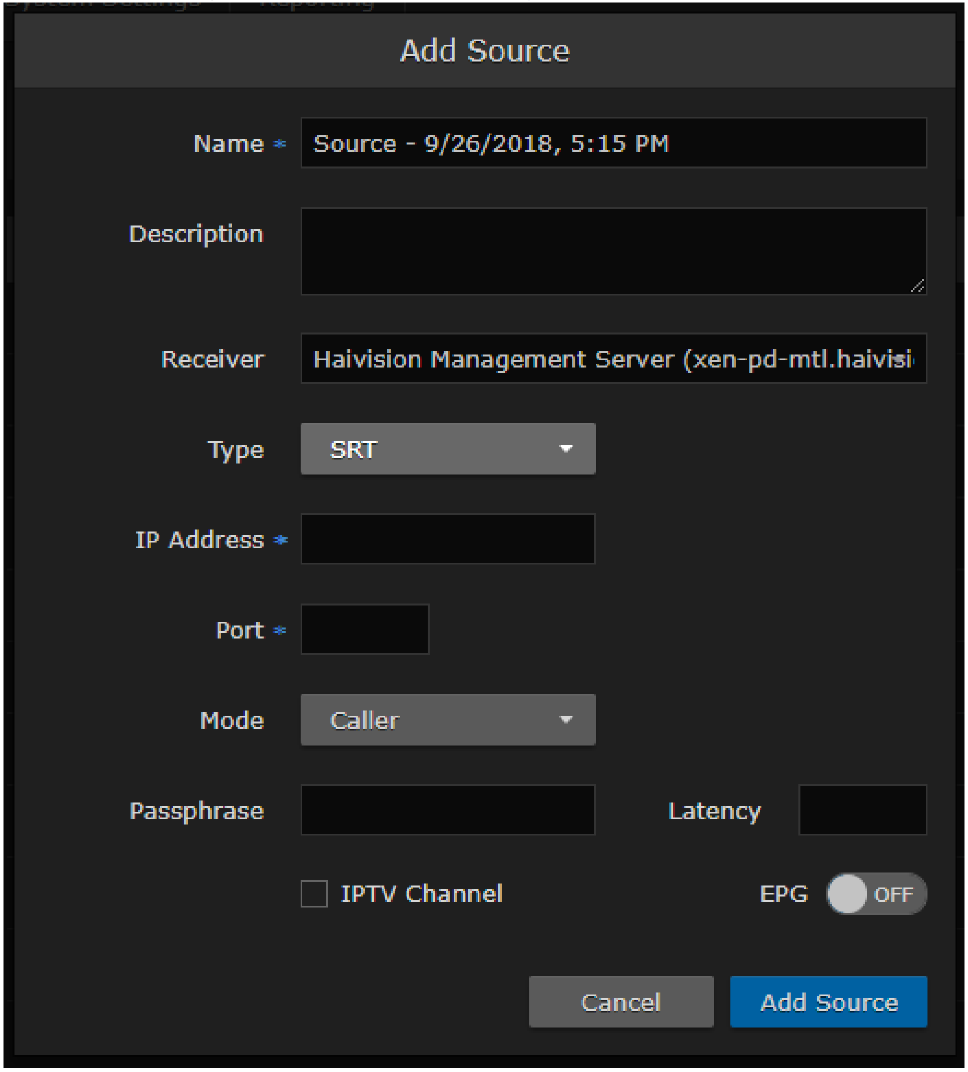
## Configuring Secure Reliable Transport (SRT) Sources

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.

For SRT-specific statistics and graphical display, see **SRT Source Statistics**.

To create an SRT connection:

1. Make sure 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**.



Add Source

Name * Source - 9/26/2018, 5:15 PM

Description

Receiver Haivision Management Server (xen-pd-mtl.haivisi

Type SRT

IP Address *

Port *

Mode Caller

Passphrase

Latency

☐ IPTV Channel

EPG OFF

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

For additional information required to set up and tune SRT streams, please see the *SRT Deployment Guide* (available through the **Haivision Support Portal** ).

## SRT Source Statistics

The following table lists the SRT Source statistics:

**Source** SRT

### Source

| Statistic | Description/Values |
|---|---|
| State | The current operating status of the source, either:<br>• Connected<br>• Disconnected<br>• Streaming<br>• Stopped<br>• Paused |
| Mode | The SRT Connection Mode. |
| Up Time | (only available when State is Connected) The length of time the source is actively streaming (dd:hh:mm:ss). |
| Bitrate | The stream bitrate (in kbps). |
| Received Packets | Number of RTP or UDP packets received for that stream. |
| Used Bandwidth | The used bandwidth in kbps. |
| Signal Losses | The number of lost signals and reconnections since the stream started. |

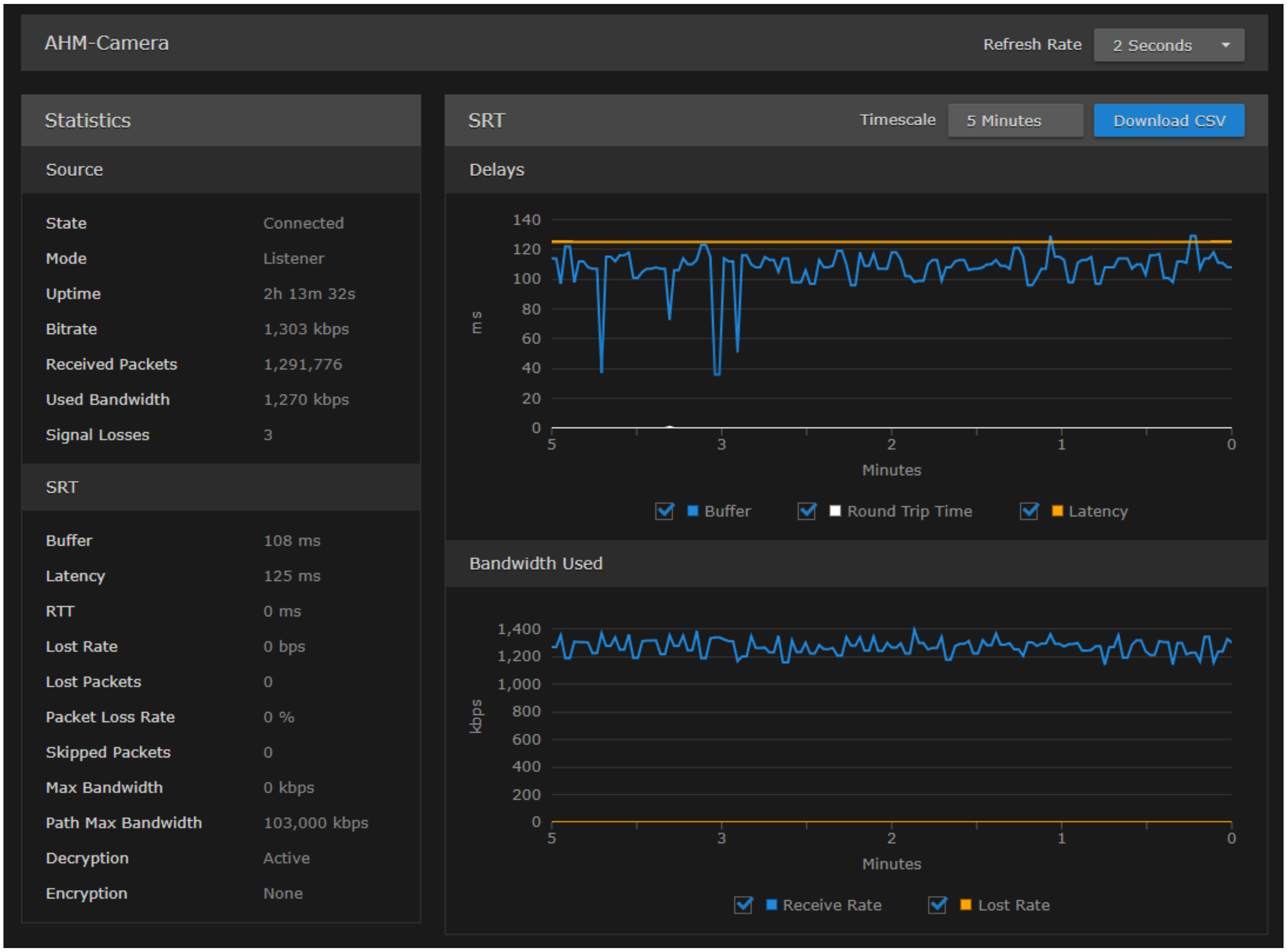
Source **SRT**

### SRT

| Statistic | Description/Values |
|---|---|
| Buffer | SRT buffer in milliseconds. Buffers are the received stream packets waiting to be transmitted. This statistic shows the portion of the buffers up to the first missing packet. In other words, the remaining time to transmit the missing packet before it's too late. The level of the buffer in absence of packet lost is just below the latency value. In presence of packets lost, it is between 0 and the latency value. |
| Latency | Maximum of the sender and receiver configured latency. For example:<br>Sender Configured SRT Latency = 750<br>Receiver Configured SRT Latency = 20<br>The SRT Stats Latency (which is the current SRT connection applied Buffering Latency) = 750 (largest of the two).<br>At startup, handshake exchanges the value configured on both sides and the largest one is selected. The receiver default is set to the minimum (20ms) so it can be completely controlled from the sender side. |
| RTT | Measured Round Trip Time (in ms). |

| Statistic | Description/Values |
|---|---|
| Lost Rate | The rate of packet loss (in bps). |
| Lost Packets | Number of SRT packets reported missing. Most are recovered. |
| Packet Loss Rate | The rate of packet loss (in packets/second). |
| Skipped Packets | Number of lost packets not recovered. |
| Max Bandwidth | Maximum bandwidth (input stream rate * (1 + overhead)). |
| Path Max Bandwidth | Maximum link bandwidth measured. This can change due to cross traffic. |
| Decryption | Indicates whether Haivision Media Platform can decrypt the stream. Either Active, Initializing, Inactive (no passphrase), or Inactive (invalid passphrase). |
| Encryption | Indicates whether AES encryption has been enabled. Either None, AES-128 or AES-256. |
| Download CSV | Click to download the statistics in CSV (“Comma Separated Value”) file format, which may be used to exchange data with applications such as Microsoft Excel. |

SRT streams include a graphical statistics display as shown in the following example:



AHM-Camera

Refresh Rate: 2 Seconds

Statistics

Source

|  |  |
|---|---|
| State | Connected |
| Mode | Listener |
| Uptime | 2h 13m 32s |
| Bitrate | 1,303 kbps |
| Received Packets | 1,291,776 |
| Used Bandwidth | 1,270 kbps |
| Signal Losses | 3 |

SRT

|  |  |
|---|---|
| Buffer | 108 ms |
| Latency | 125 ms |
| RTT | 0 ms |
| Lost Rate | 0 bps |
| Lost Packets | 0 |
| Packet Loss Rate | 0 % |
| Skipped Packets | 0 |
| Max Bandwidth | 0 kbps |
| Path Max Bandwidth | 103,000 kbps |
| Decryption | Active |
| Encryption | None |

SRT

Timescale: 5 Minutes

**Note**

Not all browsers can support the statistics graphics for SRT. You need an up-todate version of Firefox, Chrome, Safari, or IE11 (or higher) to support the graphics in the SRT Statistics page.

**Tip**

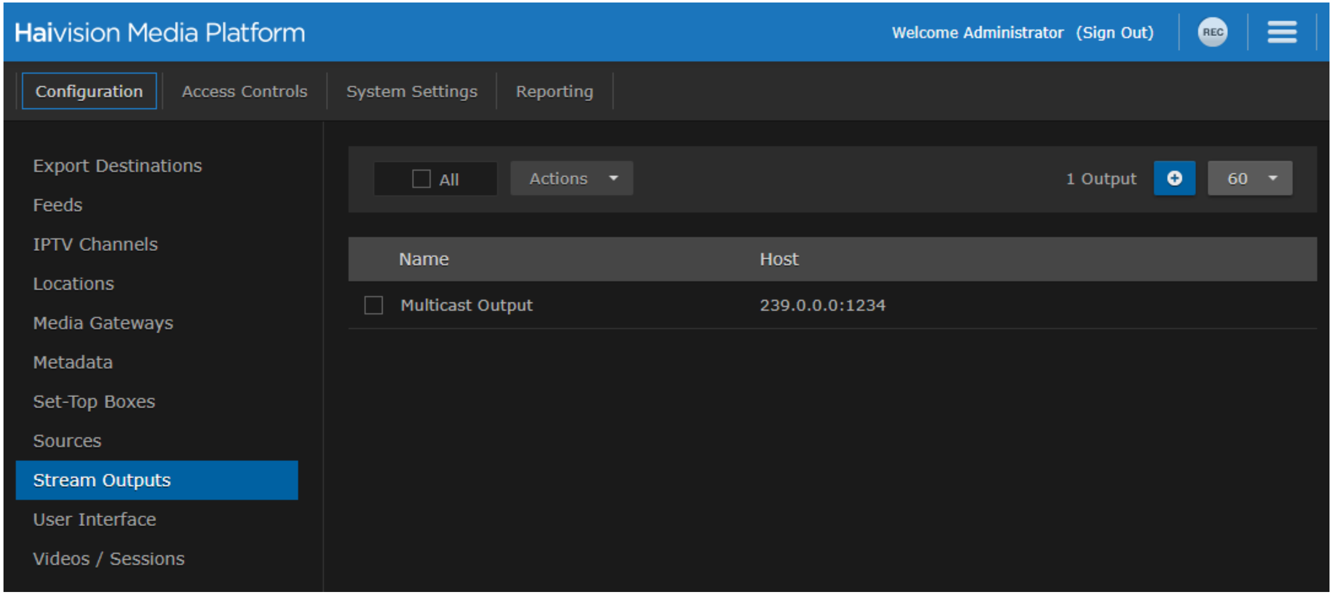
For both the Delays and Bandwidth Used displays, you can select the inputs, such as the Buffer, RTT and/or Latency, or the Receive Rate and/or Lost Rate over the time period.

## Managing Stream Outputs

When setting up Haivision Media Platform, you can define multiple stream outputs for users to select from when re-streaming videos. (Note that they can also enter 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:

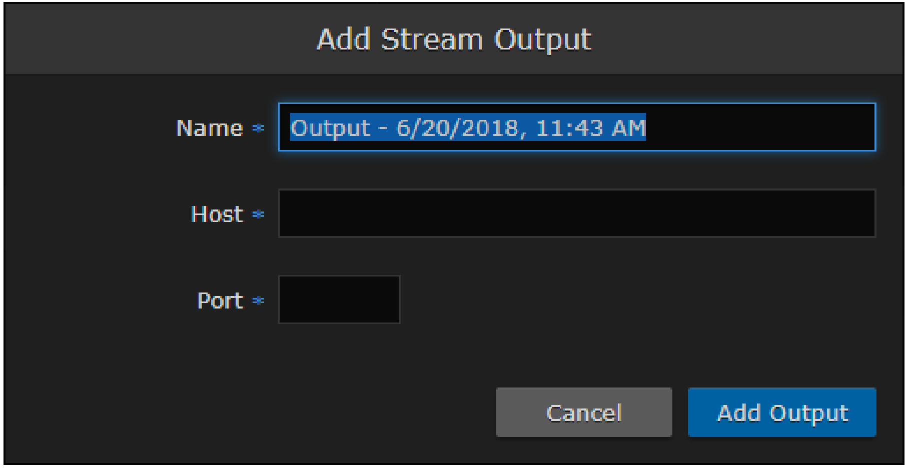
1. On the Administration screen, click **Configuration** on the toolbar and then click **Stream Outputs** on the sidebar.
   The Stream Outputs pane opens, displaying the list of defined stream outputs for your system, if any (see following example).



| Name | Host |
|---|---|
| □ Multicast Output | 239.0.0.0:1234 |

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.



Name * Output - 6/20/2018, 11:43 AM
Host *
Port *

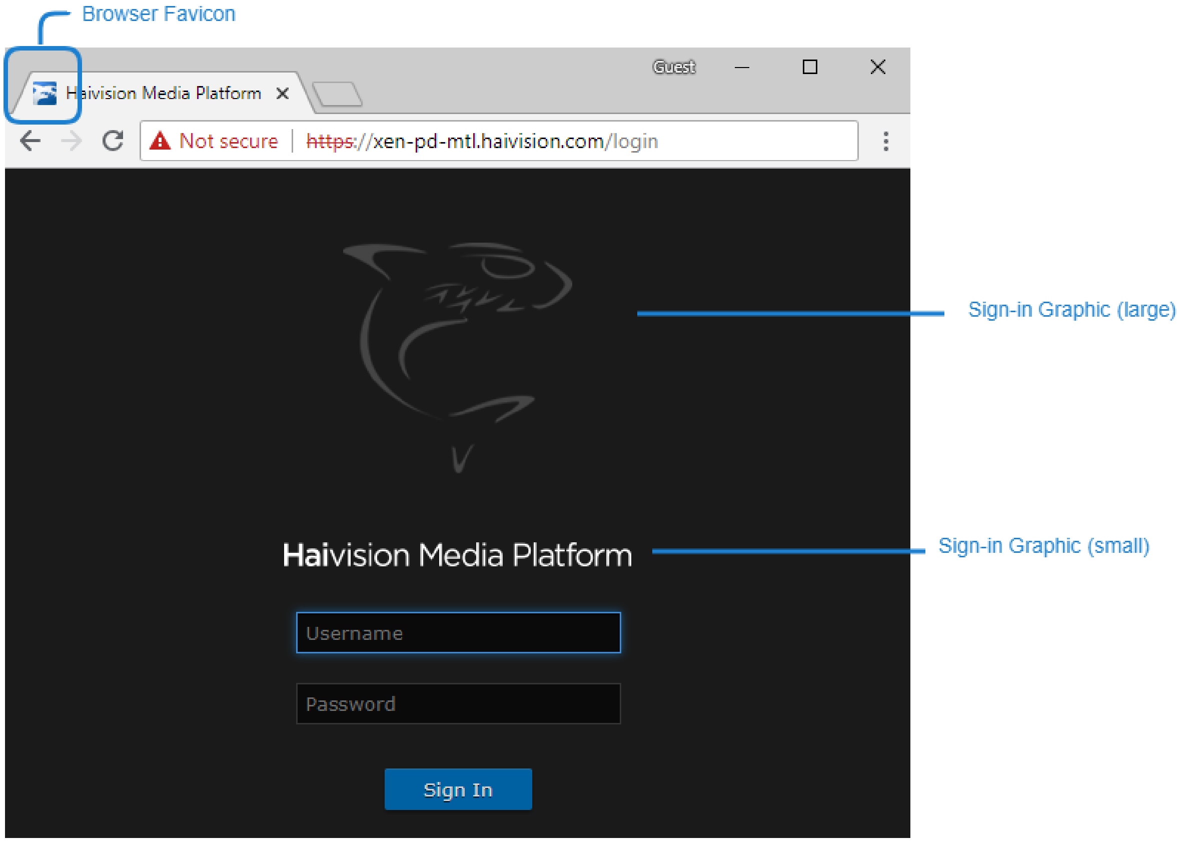
3. Click **Add Output**.
   The new output will be added to the Stream Outputs list.

## 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 will be 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.

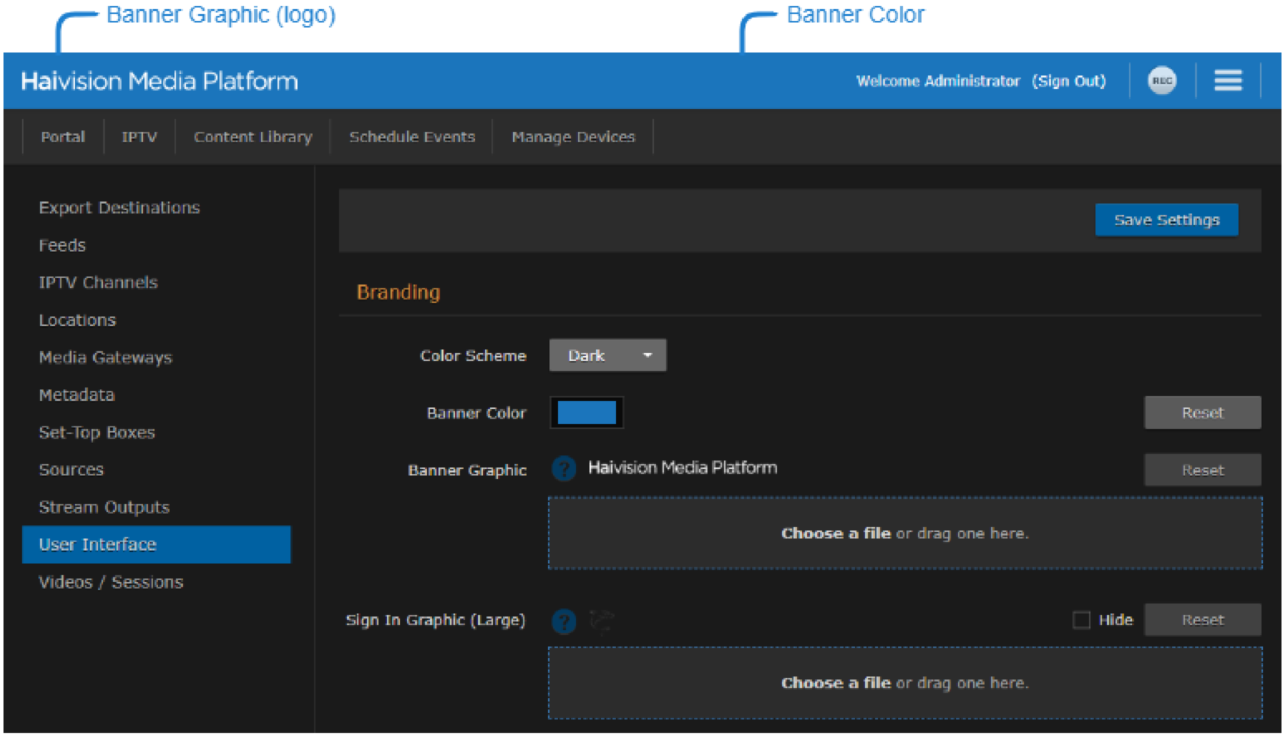
You can customize the following user interface components:

- Replace the Haivision graphics (logo and brand name) that appear on the sign-in page
- Replace the application icon that certain browsers display in the tabs and bookmarks



- Replace the Haivision banner graphic (logo) at top left of the Web interface
- Change the color of the top blue banner

- Switch color scheme between dark (default) or light



Banner Graphic (logo)

Banner Color

Branding

Color Scheme: Dark

Banner Color

Banner Graphic: Haivision Media Platform

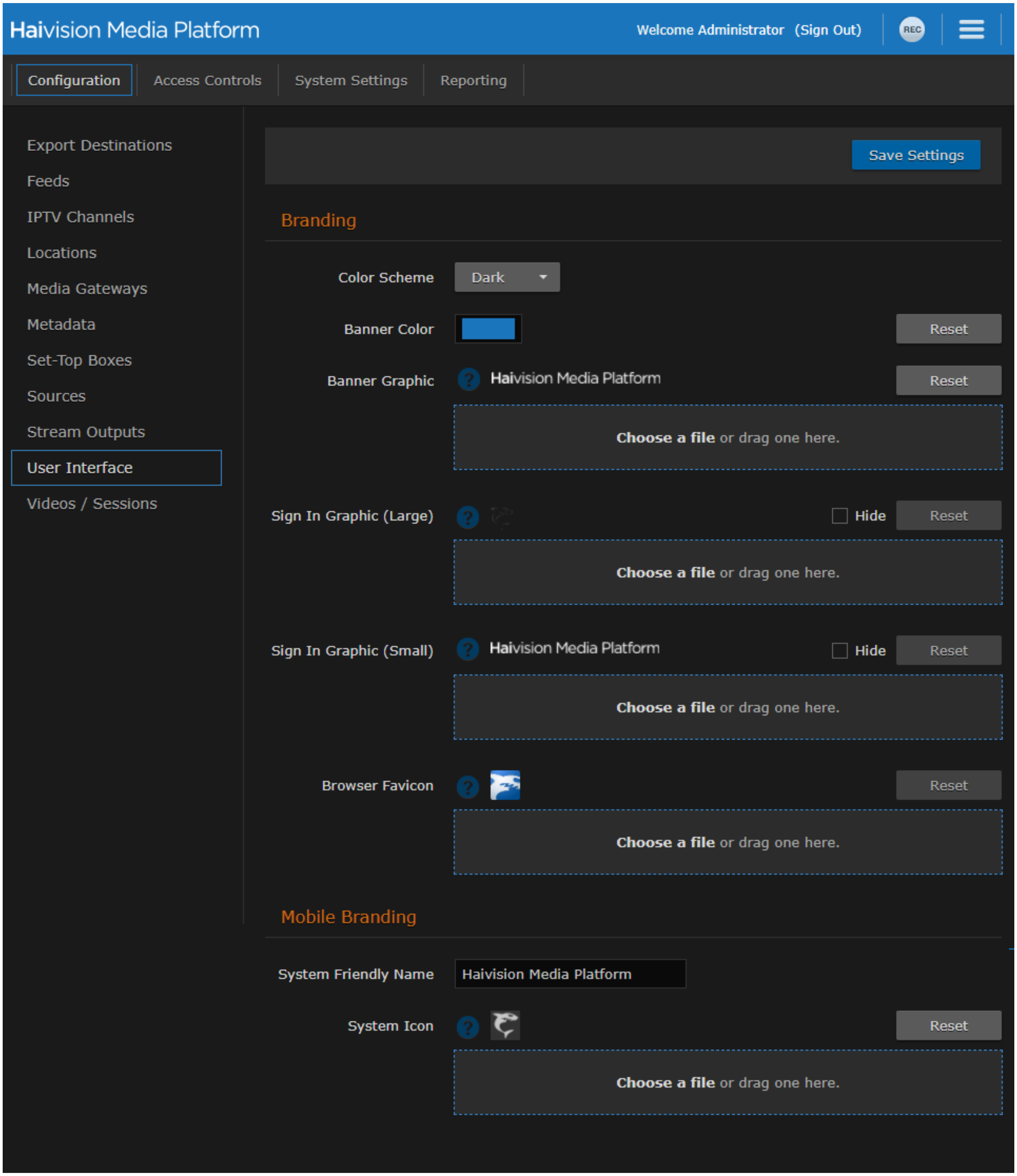
Choose a file or drag one here.

Sign In Graphic (Large) □ Hide

Choose a file or drag one here.

To customize the HMP user interface:

1. On the Administration screen, click **Configuration** on the toolbar and then click **User Interface** on the sidebar.
   The User Interface pane opens (see following example).



Branding

Color Scheme: Dark

Banner Color

Banner Graphic: Haivision Media Platform

Sign In Graphic (Large) □ Hide

Sign In Graphic (Small): Haivision Media Platform □ Hide

Browser Favicon

Mobile Branding

System Friendly Name: Haivision Media Platform

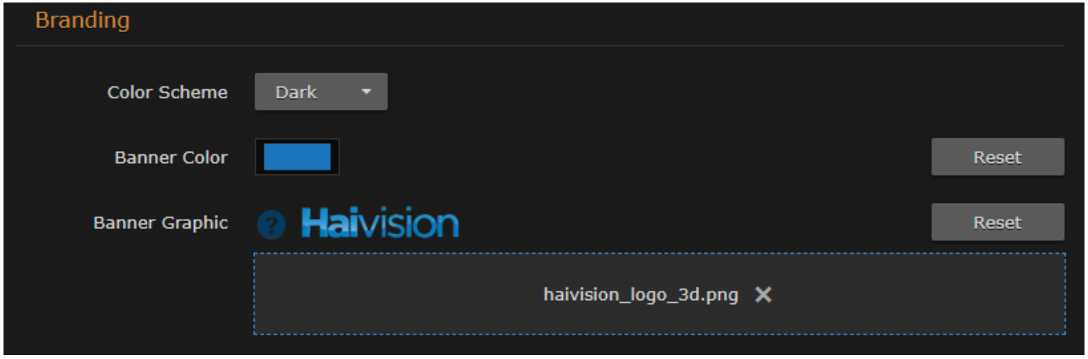
System Icon

2. To switch the interface color scheme between dark (default) and light, select from the Color Scheme drop-down menu.
3. To change the banner color, click the color box and select the new color (either directly from the color picker or enter the color values).

4. **Tip**

   To view the expected dimensions for an image, hover the cursor over the ? icon.

5. Drag an image to the drop area or click **Choose a file** to choose the new graphic. The image and the filename are displayed (as shown in the following example).



Branding

Color Scheme: Dark

Banner Color

Banner Graphic

haivision_logo_3d.png

**Tip**

To revert to the default image or banner color, click **Reset**.

6. To hide one of the Sign-In page graphics (large or small), check the Hide checkbox. To show it again, choose a new graphic or uncheck the checkbox.
7. 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.)

Branding Mobile Branding

### Branding

| Setting | Default | Description/Values |
|---|---|---|
| Color Scheme | Dark | Switch interface between dark and light color schemes<br>• Dark: black background with white text (default)<br>-or-<br>• 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. |
| Banner Graphic | Haivision Media Platform (text logo) | **Tip**<br>The Haivision graphic is a 235 x 16 pixel .PNG file. |
| Sign-in Graphic (large) | Haivision shark logo | **Note**<br>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 will be cut off. The image is centered horizontally.<br>**Tip**<br>The Haivision graphic is a 156 x 206 pixel .PNG file. |
| Sign-in Graphic (small) | Haivision Media Platform (text logo) | The lower image on the Sign-in page. The width and height can be any dimension to fit the page. However, the image will be 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 | **Tip**<br>The width and height can be 16, 32, 48 or 64 pixels (squared), 8-bit or 24-bit. |

Branding Mobile Branding

### Mobile Branding

**Tip**

Mobile Branding settings can also be set locally from the Play Mobile 2.0.2 app.

| Setting | Default | Description/Values |
|---|---|---|
| System Friendly Name | Haivision Media Platform | Used to identify the HMP system by name on a Play Mobile device. |
| System Icon | Haivision mobile system icon | **Tip**<br>The width and height should be a 132px square (maximum 512 px). |

# 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.

## Default Video Expiry

The Default Video Expiry specifies the number of days after which a video will expire and be deleted. Alternatively, you can select "Keep Forever", so that videos will *not* be deleted automatically. The minimum expiration is one (1) day.

**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.

**When editing Video information, 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).**

## Maximum Recording Duration

Each recording session is limited to a maximum duration. HMP stops recording when reaching that duration. You can define the maximum duration for all videos. The default is 24 hours.

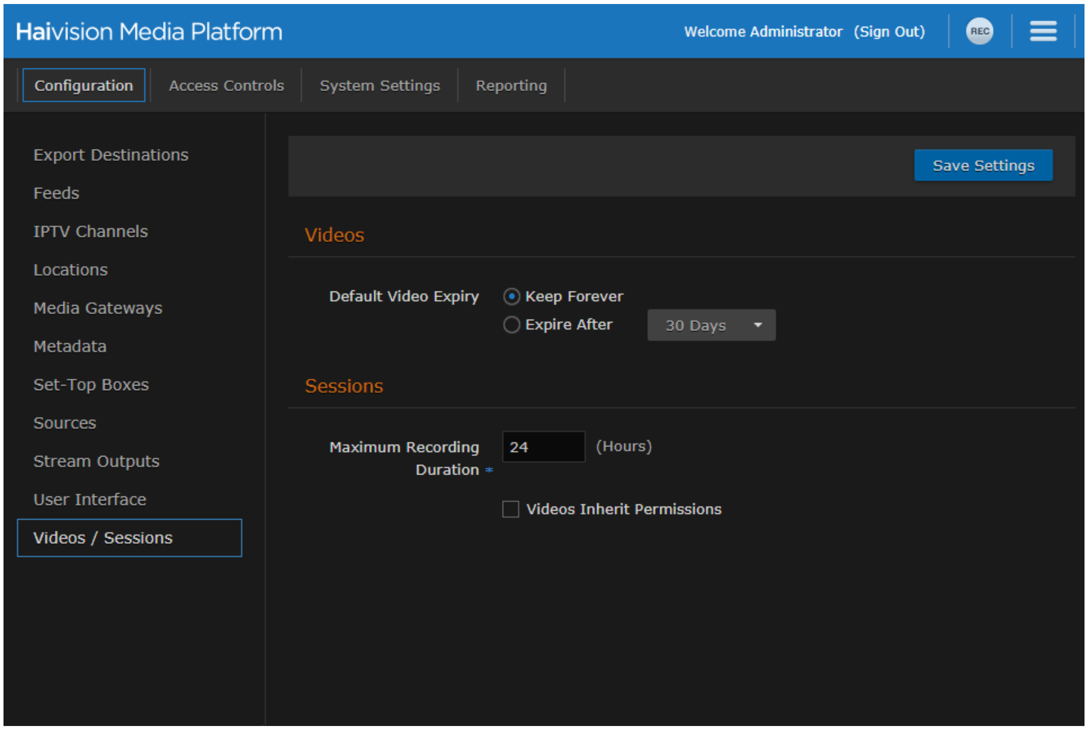
## Videos Inherit Permissions

A session's sharing permissions may be passed to any videos made from that session. The objective is a workflow decision to help reduce the number of times a user must enter the sharing dialog.

Administrators can enable or disable (default) this setting. Permissions are copied at the start of the recording. The recording creator is still granted "OWN" permissions on the new video.

To configure the video and session settings:

1. On the Administration screen, click **Configuration** on the toolbar and then click **Videos/Sessions** on the sidebar.
   The Videos / Sessions pane opens (see following example).



Videos

Default Video Expiry ● Keep Forever

○ Expire After 30 Days

Sessions

Maximum Recording Duration * 24 (Hours)

□ Videos Inherit Permissions

2. For the Default Video Expiry, select either **Keep Forever** or **Expire After**.
3. For Expire After, select a duration from the Days drop-down menu (ranging from 1 – 180 days).
4. To change the Maximum Recording Duration, type in the number of hours.
   To allow a session's sharing permissions to be passed on to videos made from that session (disabled by default), check the **Videos Inherit Permissions – Activate** checkbox.
5. Click **Save Settings**.

# Managing Access Controls

**Important**

Before proceeding, make sure that:

- The appliance is set up correctly and all necessary network and A/V connections are established. For information on installing and connecting to your Haivision Media Platform server, please refer to the **Server Quick Start Guide - Issue 01**.
- 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

**Important**

If HMP is connected to an LDAP or Active Directory server, the Users list will be 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.**

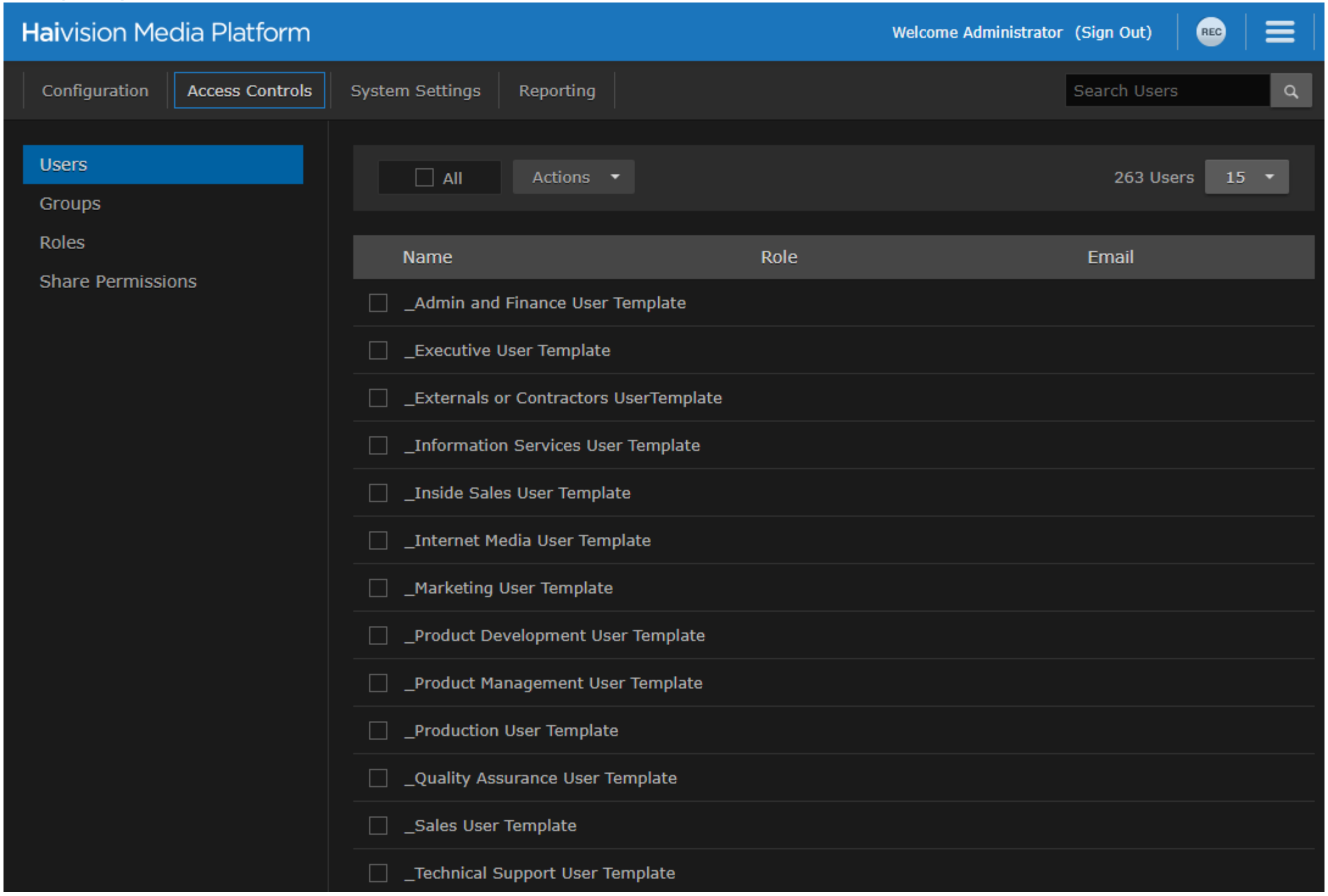
If your system is *not* connected to a directory server, you may also add and modify user accounts from HMP.

**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:**

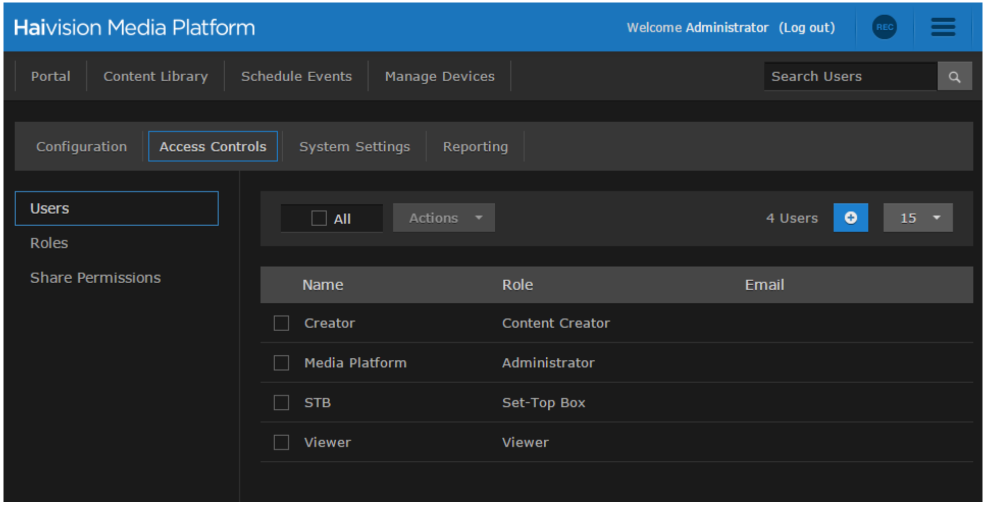
1. To navigate the Administration screen, click the ☰ icon on the banner and select **Administration** from the navigation drop-down menu.
2. On the Administration screen, click **Access Controls** on the toolbar and then click **Users** on the sidebar.
   The Users list opens, displaying the list of defined users for your platform.
3. In an LDAP/AD environment, you may browse through the list and assign roles to users. See Assigning Roles to LDAP/AD Users.



| | Name | Role | Email |
|---|---|---|---|
| □ | _Admin and Finance User Template | | |
| □ | _Executive User Template | | |
| □ | _Externals or Contractors UserTemplate | | |
| □ | _Information Services User Template | | |
| □ | _Inside Sales User Template | | |
| □ | _Internet Media User Template | | |
| □ | _Marketing User Template | | |
| □ | _Product Development User Template | | |
| □ | _Product Management User Template | | |
| □ | _Production User Template | | |
| □ | _Quality Assurance User Template | | |
| □ | _Sales User Template | | |
| □ | _Technical Support User Template | | |

-or-

4. 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).



| Name | Role | Email |
|---|---|---|
| □ Creator | Content Creator | |
| □ Media Platform | Administrator | |
| □ STB | Set-Top Box | |
| □ Viewer | Viewer | |

**Note**

Starting with Release 3.0, on new installations, the default HMP users (non LDAP/AD) are operator and user.

### Topics Discussed

- Assigning Roles to LDAP/AD Users
- Managing User Accounts (Non LDAP/AD)
- User Settings

## Assigning Roles to LDAP/AD Users

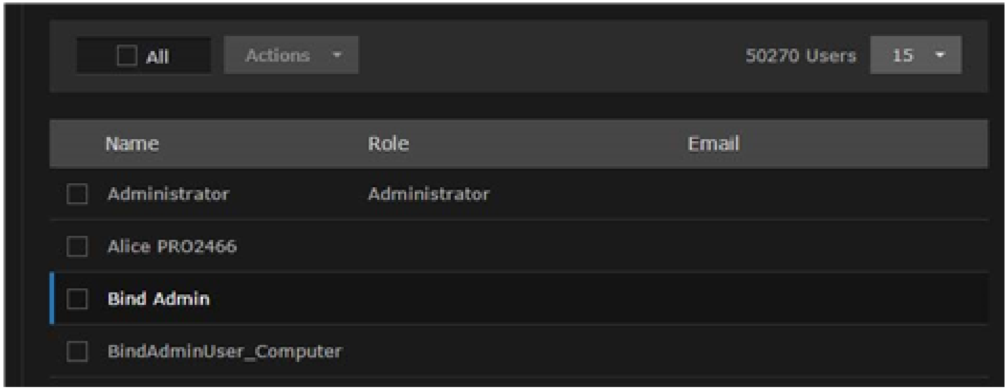
**Important**

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:**

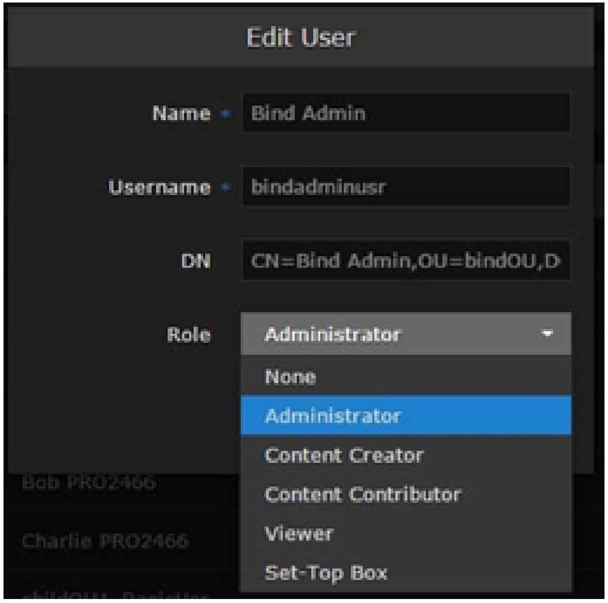
1. Select the user by mousing over the user name in the Users list and click anywhere in the row.



| | Name | Role | Email |
|---|---|---|---|
| ☐ | Administrator | Administrator | |
| ☐ | Alice PRO2466 | | |
| ☐ | Bind Admin | | |
| ☐ | BindAdminUser_Computer | | |

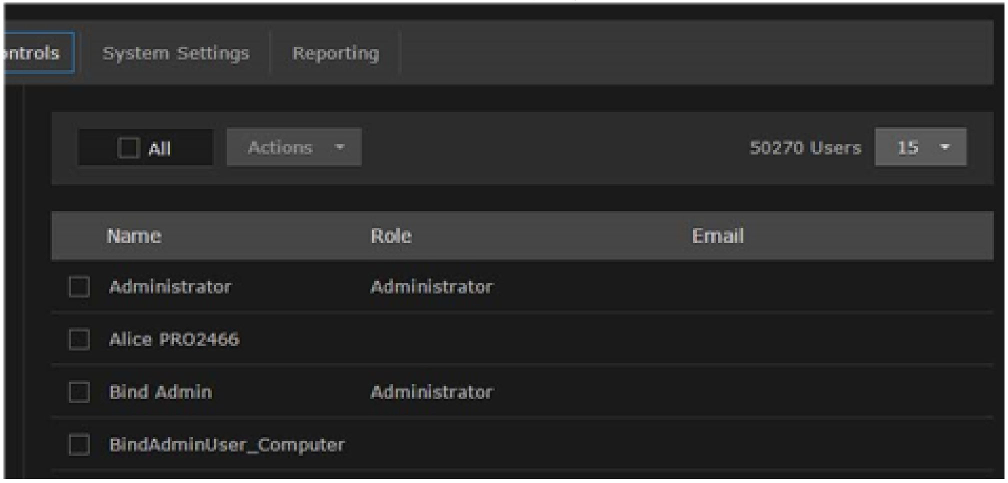
   Or you can check the checkbox next to the user name and click **Edit**.

2. On the Edit User dialog, select the role for the user account. See the Role entry in User Settings.



| | |
|---|---|
| Name * | Bind Admin |
| Username * | bindadminusr |
| DN | CN=Bind Admin,OU=bindOU,D |
| Role | Administrator ▾ |

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



| Name | Role | Email |
|---|---|---|
| □ Administrator | Administrator | |
| □ Alice PRO2466 | | |
| □ Bind Admin | Administrator | |
| □ BindAdminUser_Computer | | |

**Related Topics**

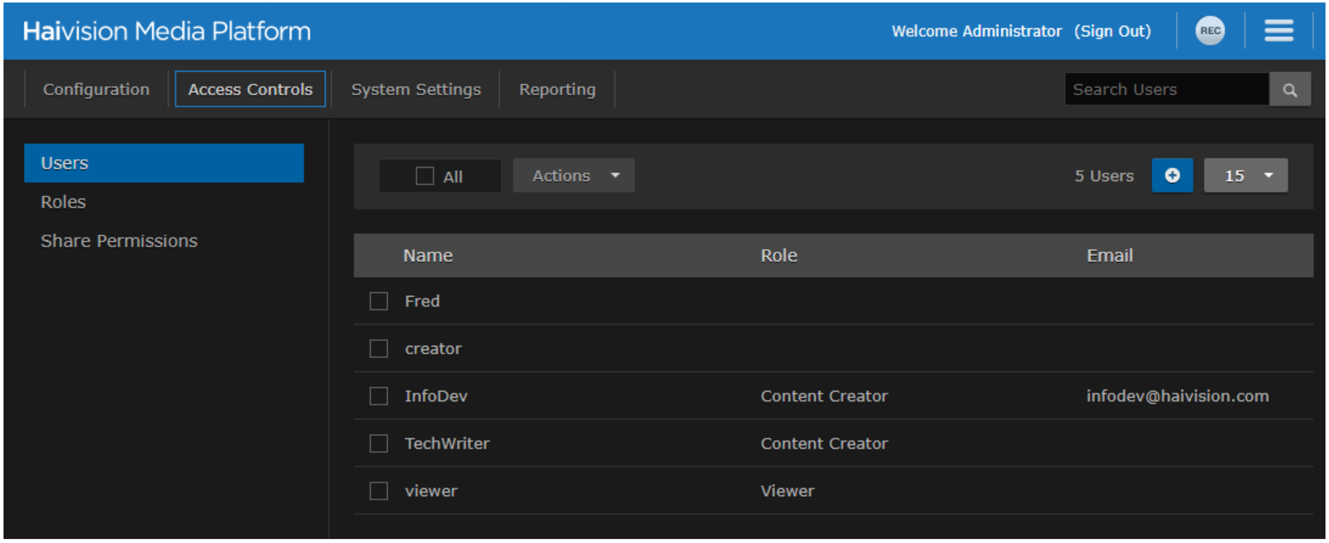
- User Settings

## Managing User Accounts (Non LDAP/AD)

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

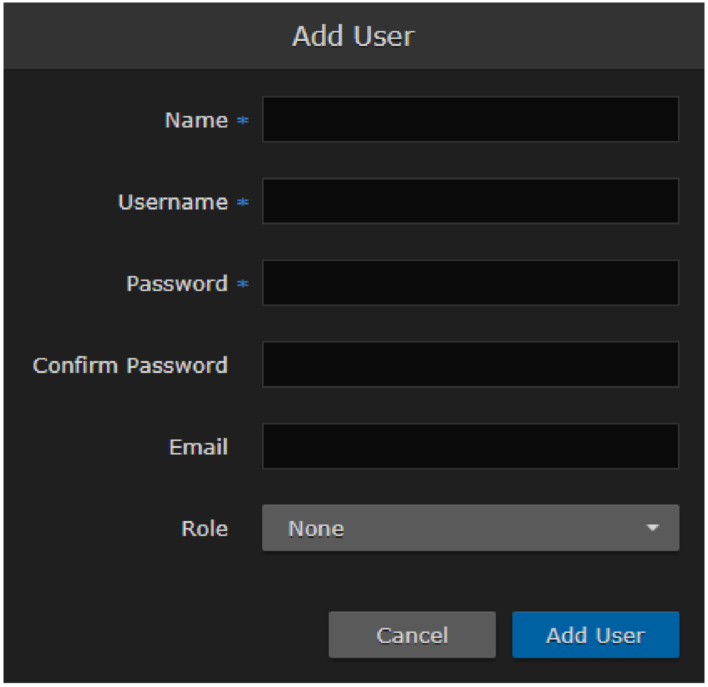
To add a user:

1. From the Users list (Administration screen), click the ⊕ icon.



| Name | Role | Email |
|---|---|---|
| □ Fred | | |
| □ creator | | |
| □ InfoDev | Content Creator | infodev@haivision.com |
| □ TechWriter | Content Creator | |
| □ viewer | Viewer | |

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



Add User

Name *

Username *

Password *

Confirm Password

Email

Role None

3. Click **Add User**. The new user will be 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 | n/a | Enter a name for the user. This name will be displayed on the Users list. |
| Username | n/a | **Note**<br>You cannot modify the username. |
| Password | n/a | Type in the new password. |
| Confirm Password | n/a | Type in the new password again. |
| Email | n/a | Enter an email address to associate with the user account. |
| Role | None | **Note**<br>For information on creating and customizing roles for your system, see Managing Roles.<br>For the default role permissions, see Default Roles. |

# Managing Groups (LDAP/AD Only)

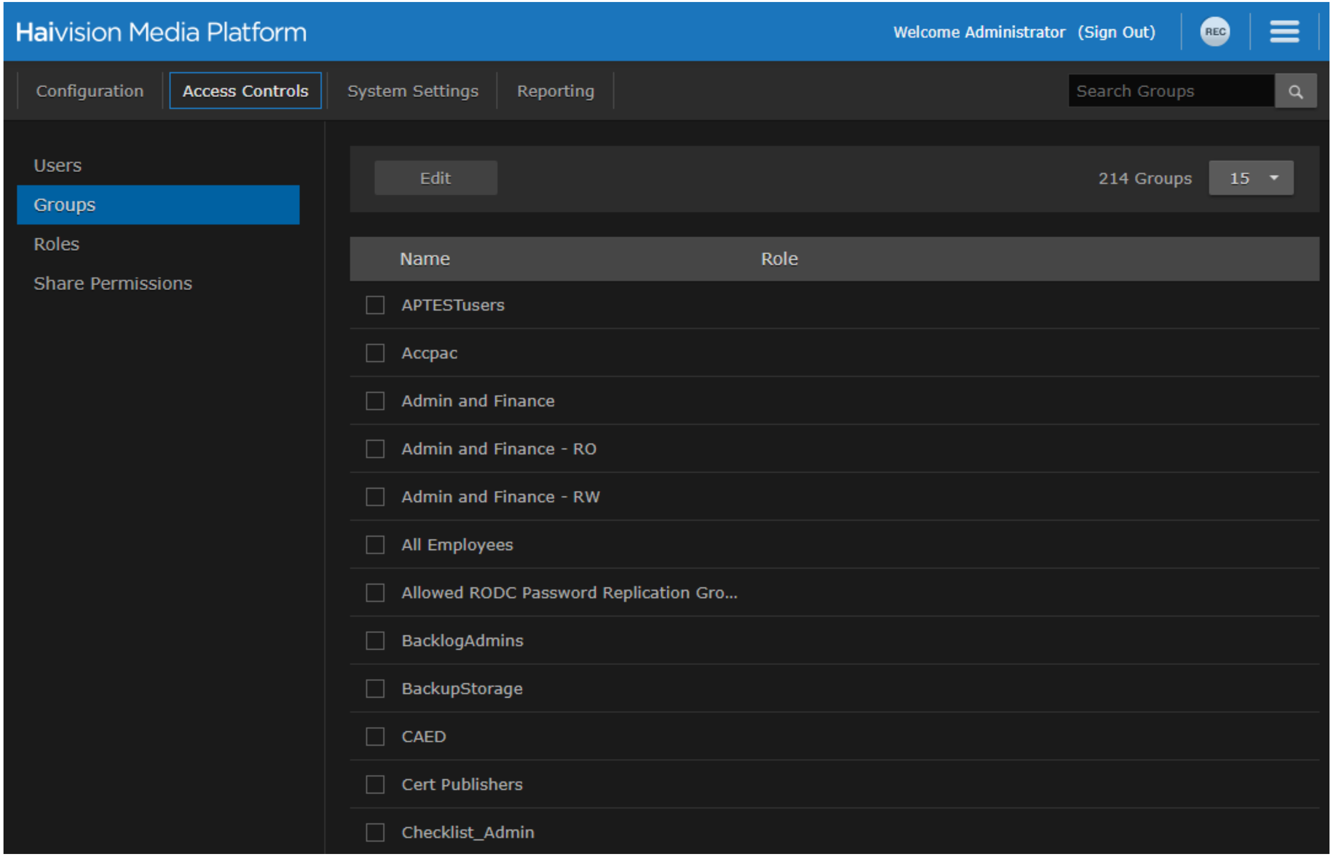
**Important**

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 will be 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. On the Administration screen, 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).



| | Name | Role |
|---|---|---|
| □ | APTESTusers | |
| □ | Accpac | |
| □ | Admin and Finance | |
| □ | Admin and Finance - RO | |
| □ | Admin and Finance - RW | |
| □ | All Employees | |
| □ | Allowed RODC Password Replication Gro... | |
| □ | BacklogAdmins | |
| □ | BackupStorage | |
| □ | CAED | |
| □ | Cert Publishers | |
| □ | Checklist_Admin | |

2. To assign roles to groups, see Assigning Roles to LDAP/AD Groups.

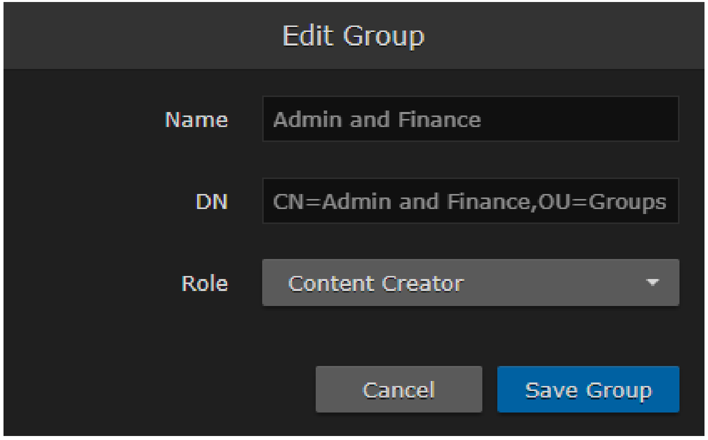
## Assigning Roles to LDAP/AD Groups

**Important**

If Haivision Media Platform is connected to an LDAP or Active Directory server, the HMP Groups list will be 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**.



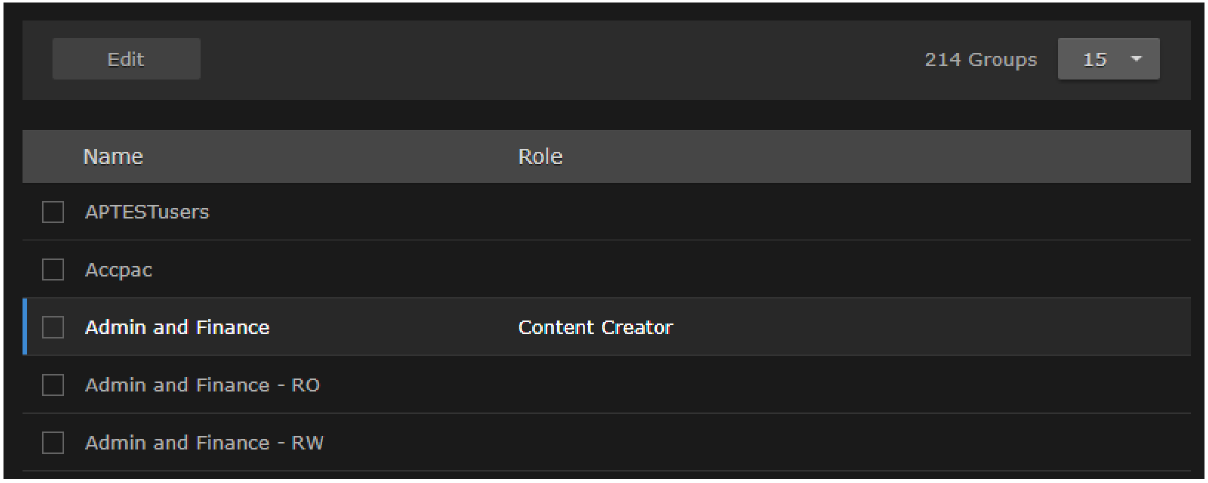
Edit Group

Name: Admin and Finance

DN: CN=Admin and Finance,OU=Groups

Role: Content Creator

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



| | Name | Role |
|---|---|---|
| □ | APTESTusers | |
| □ | Accpac | |
| □ | Admin and Finance | Content Creator |
| □ | Admin and Finance - RO | |
| □ | Admin and Finance - RW | |

# Managing Roles

*Roles* are used to confer permissions to users and groups. A user must be assigned a role in order 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 "share" permissions for content rights (videos, sessions and sources) by administrators or other users. Share permissions may further qualify a user's privileges.**

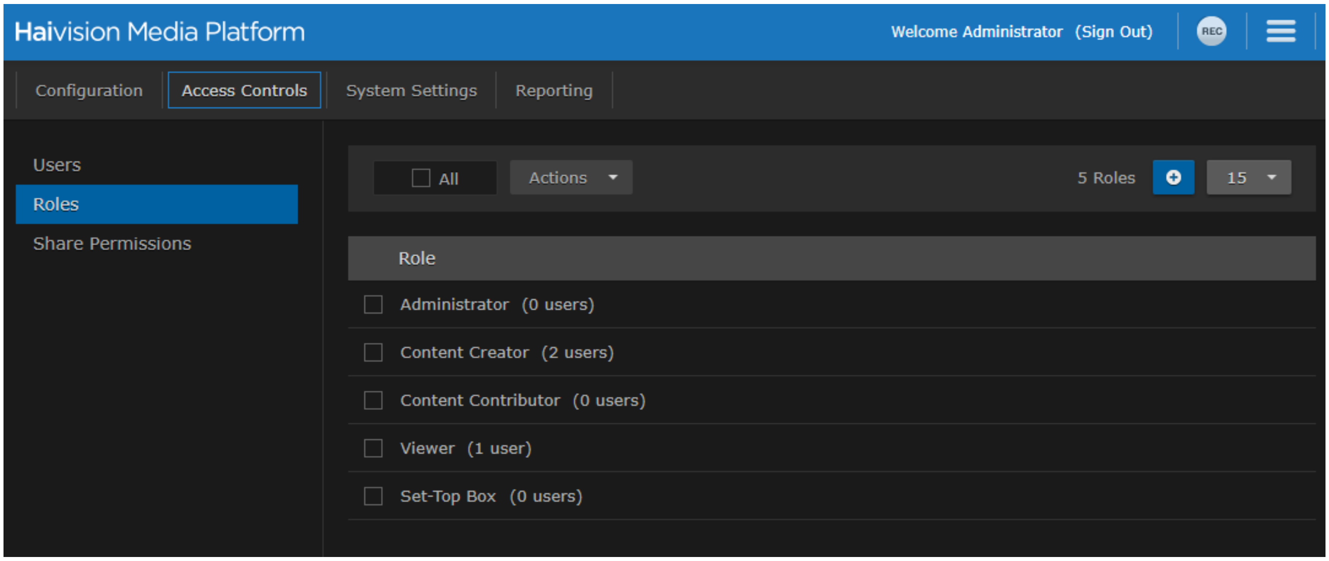
HMP roles and share permissions are fully customizable (see **Creating Custom Roles** and **Managing Share Permissions**).

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



| Role |
|---|
| □ Administrator (0 users) |
| □ Content Creator (2 users) |
| □ Content Contributor (0 users) |
| □ Viewer (1 user) |
| □ Set-Top Box (0 users) |

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, see **Editing Role Permissions**
- To create new roles, see **Creating Custom Roles**
- To delete roles, see **Deleting Items**

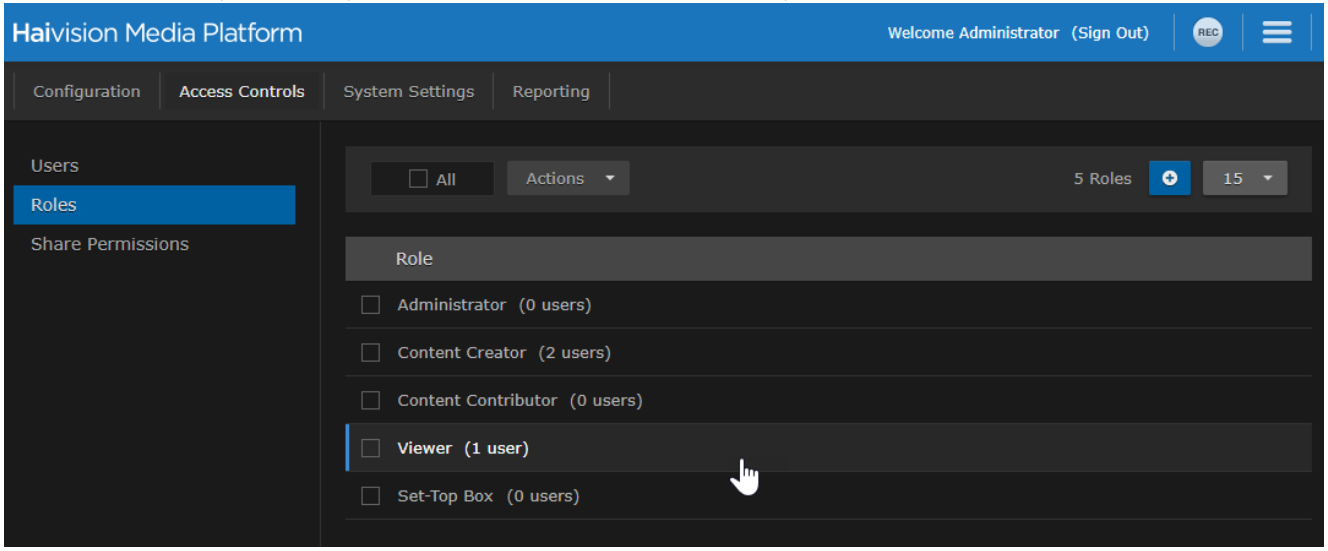
### Related Topics

- **Default Roles**

## Adding Users and Groups to Roles

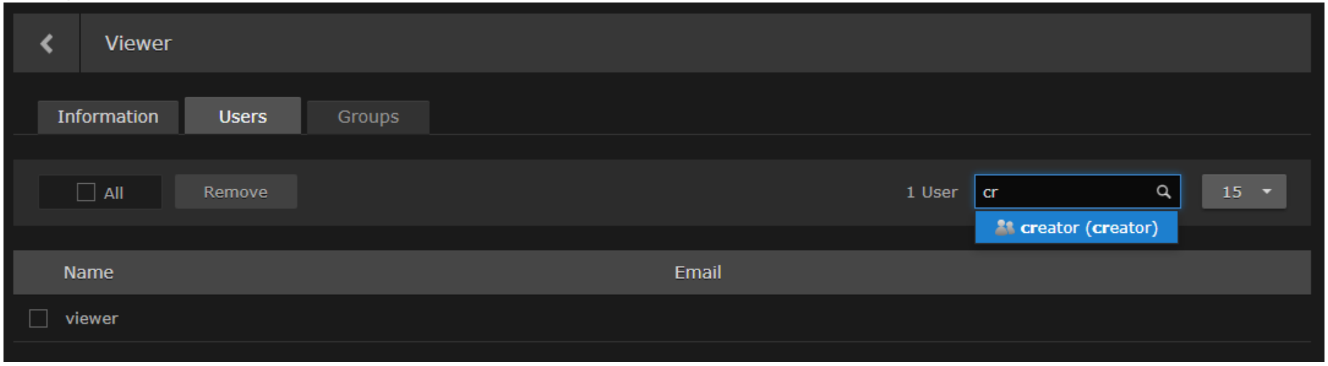
To add users and/or groups to a role:

1. Select the role by hovering over the role name and click anywhere in the row.



□ Administrator (0 users)
□ Content Creator (2 users)
□ Content Contributor (0 users)
□ Viewer (1 user)
□ Set-Top Box (0 users)

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.



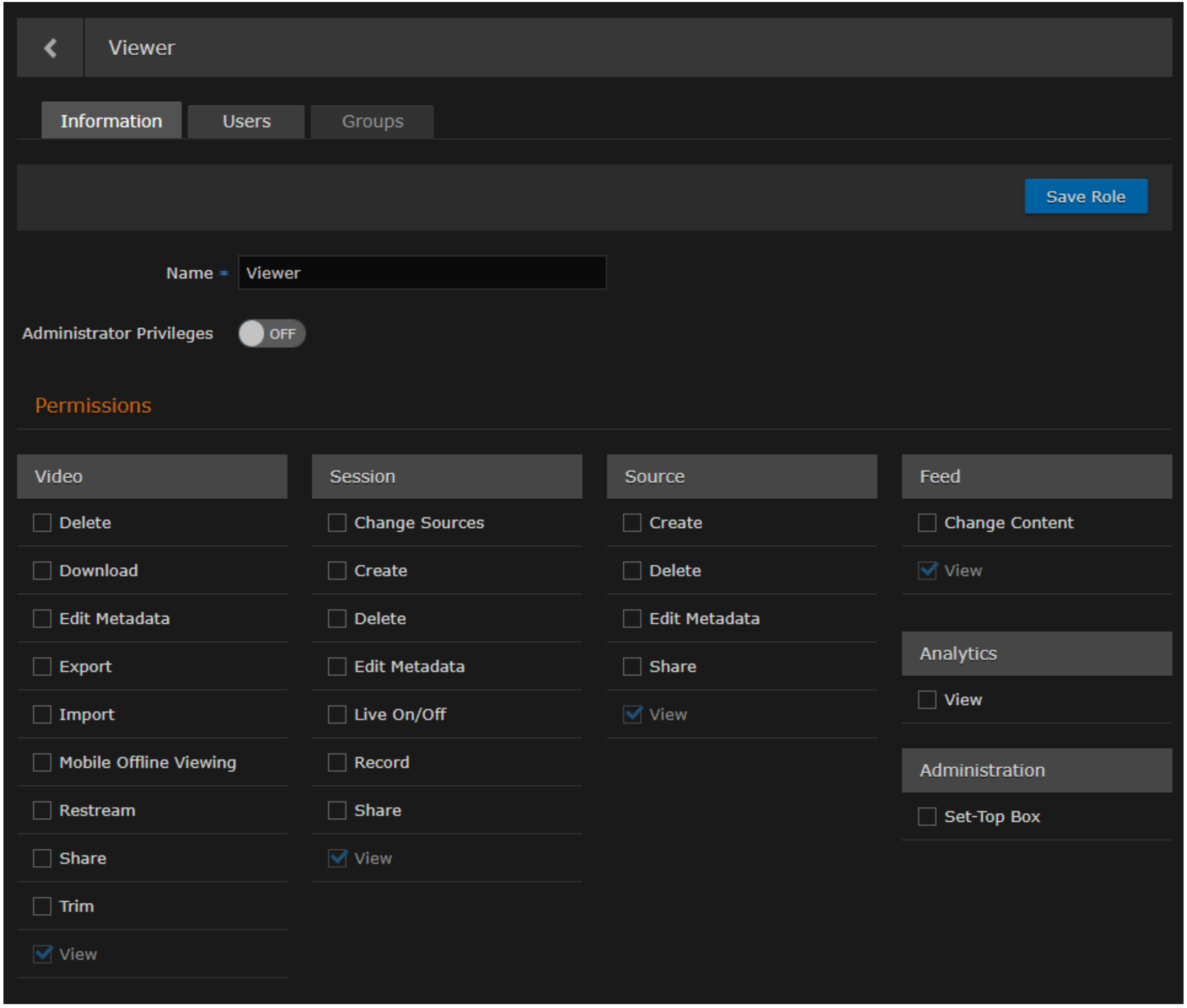
| Name | Email |
|---|---|
| □ viewer | |

4. Select the user or group from the list that appears. The selected user or group is now added to the role (see following example).
5. Click the ‹ icon to return to the Roles list.

## Editing Role Permissions

To edit permissions for a role:

1. Select the role in the Roles list.
2. On the Information pane, check or uncheck the permissions as required.



Viewer

Name * Viewer

Administrator Privileges OFF

Permissions

Video
- □ Delete
- □ Download
- □ Edit Metadata
- □ Export
- □ Import
- □ Mobile Offline Viewing
- □ Restream
- □ Share
- □ Trim
- ☑ View

Session
- □ Change Sources
- □ Create
- □ Delete
- □ Edit Metadata
- □ Live On/Off
- □ Record
- □ Share
- ☑ View

Source
- □ Create
- □ Delete
- □ Edit Metadata
- □ Share
- ☑ View

Feed
- □ Change Content
- ☑ View

Analytics
- □ View

Administration
- □ Set-Top Box

**Tip**

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

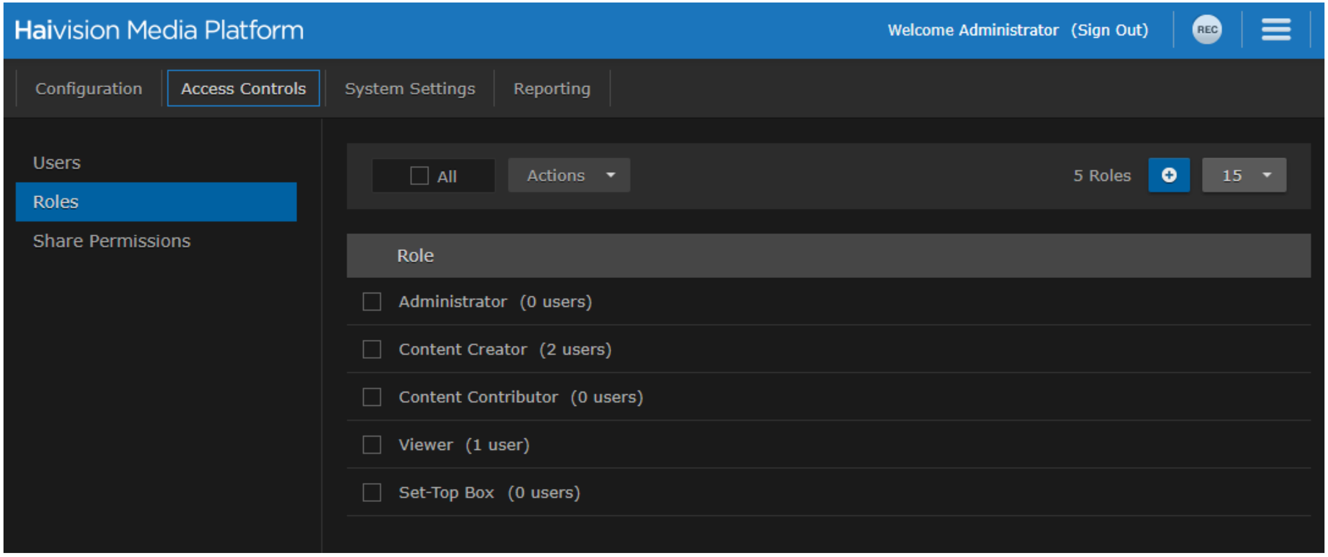
3. Click **Save Role**. The selected permissions will be applied to the role.

## 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.

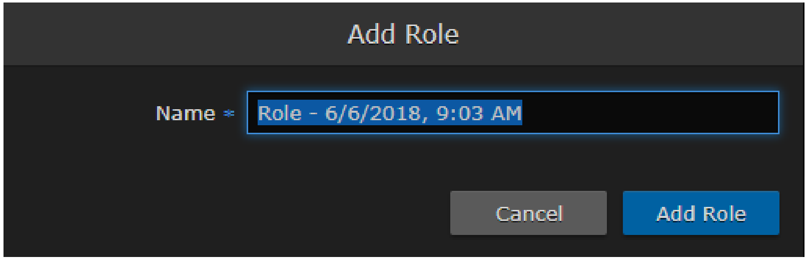
To create a custom role:

1. From the Roles list, click the ⊕ icon.



- □ Administrator (0 users)
- □ Content Creator (2 users)
- □ Content Contributor (0 users)
- □ Viewer (1 user)
- □ Set-Top Box (0 users)

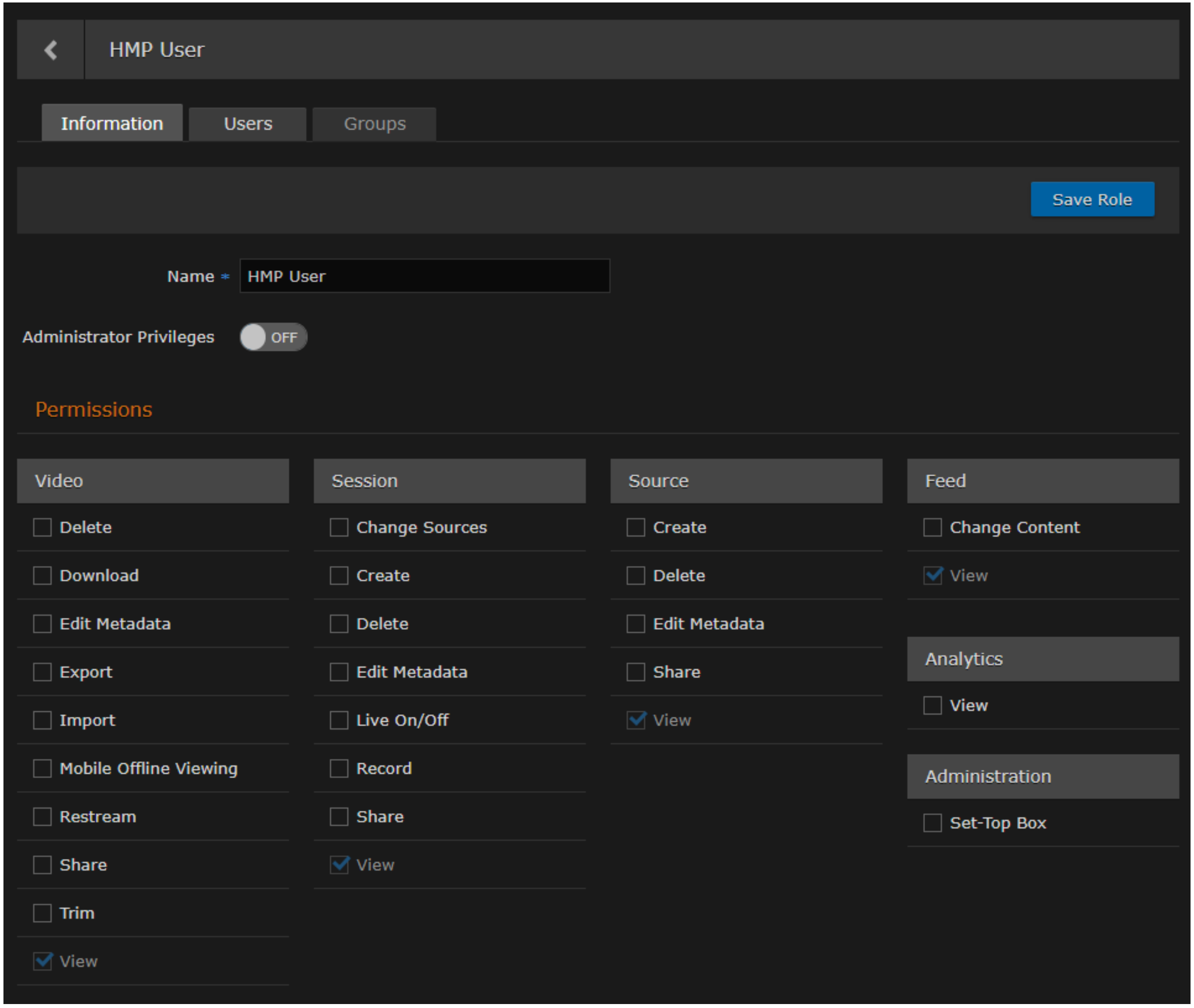
2. On the Add Role Information dialog, type in a name for the role.



Name * Role - 6/6/2018, 9:03 AM

3. Click **Add Role**.

4. On the Information pane, check the permissions to assign to the role. Note that “View” is always enabled for Video, Session, Source and Feed permissions.



Name * HMP User

Administrator Privileges OFF

Permissions

Video
- ☐ Delete
- ☐ Download
- ☐ Edit Metadata
- ☐ Export
- ☐ Import
- ☐ Mobile Offline Viewing
- ☐ Restream
- ☐ Share
- ☐ Trim
- ☑ View

Session
- ☐ Change Sources
- ☐ Create
- ☐ Delete
- ☐ Edit Metadata
- ☐ Live On/Off
- ☐ Record
- ☐ Share
- ☑ View

Source
- ☐ Create
- ☐ Delete
- ☐ Edit Metadata
- ☐ Share
- ☑ View

Feed
- ☐ Change Content
- ☑ View

Analytics
- ☐ View

Administration
- ☐ Set-Top Box

**Tip**

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

**Important**

Administrators may create additional roles as well as edit the permissions for the default roles. Role permissions may be further qualified by "share" 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 Feeds Analytics Administration

### Videos

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

Videos Sessions Sources Feeds Analytics Administration

### Sessions

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

Videos Sessions Sources Feeds Analytics Administration

### Sources

| Tasks | Roles | | | | |
|---|---|---|---|---|---|
| | Administrator | Content Creator | Content Contributor | Viewer | Set-Top Box |
| Create Sources | ✓ | OWN | OWN | OWN | |
| Delete Sources | ✓ | OWN | OWN | OWN | |
| Edit Metadata | ✓ | EDIT | EDIT | EDIT | |
| Share Sources | ✓ | OWN | OWN | OWN | |
| View Sources | ✓ | ✓ | ✓ | ✓ | ✓ |

Videos Sessions Sources Feeds Analytics Administration

### Feeds

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

Videos Sessions Sources Feeds Analytics Administration

### Analytics

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

Videos Sessions Sources Feeds Analytics Administration

### Administration

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

## Managing Share Permissions

**Note**

Users can share items such as feeds, sources, videos, and sessions with other users or groups. Sharing is defined on the Content Library Share pane (by clicking the **Share** tab from the Information pane when setting up or editing an item). You can specify access permissions on a per-user or per-group basis.
For information on the default share permissions and the steps to share feeds, sources, videos, and sessions, see Sharing Items (in the User's Guide).

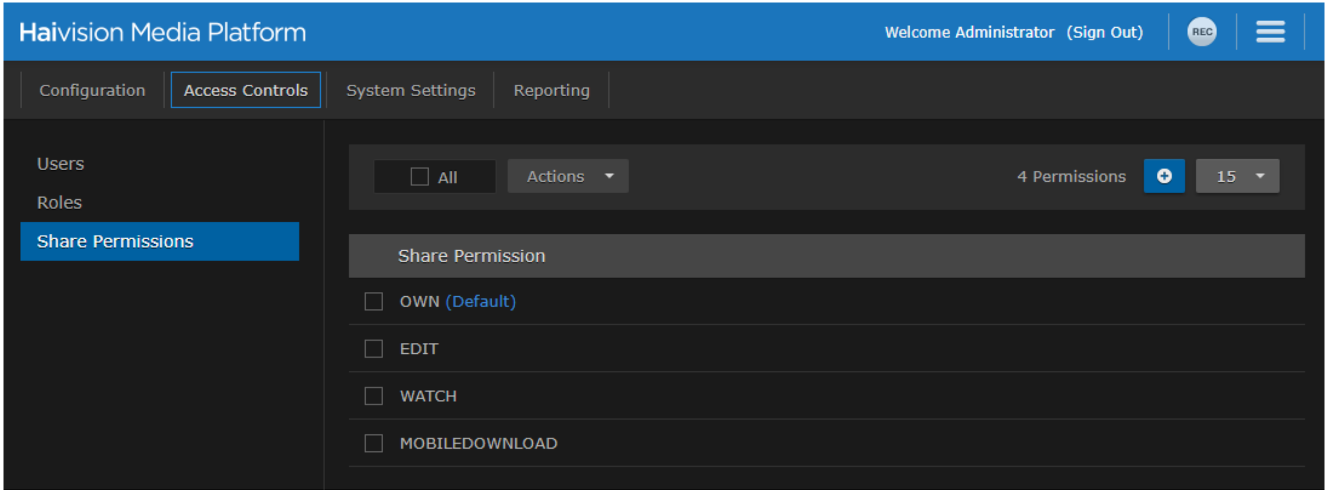
Administrators and other users may assign users "share" permissions for content rights (videos, sessions, sources, and feeds). Share permissions are combined with a user's role and may further qualify the user's privileges.

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

> **Important**
>
> Once an asset is selected for a feed, the feed share 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.

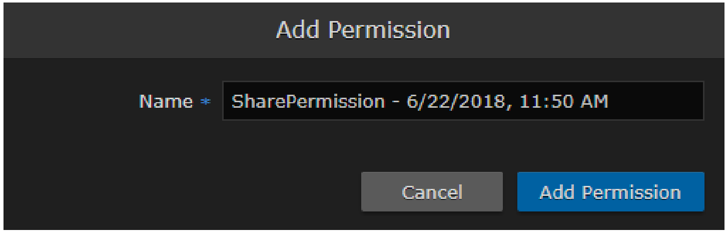
To view and manage share permissions:

1. On the Administration screen, click **Access Controls** on the toolbar and then click **Share Permissions** on the sidebar.
   The Share Permissions list opens, as shown in the following example.



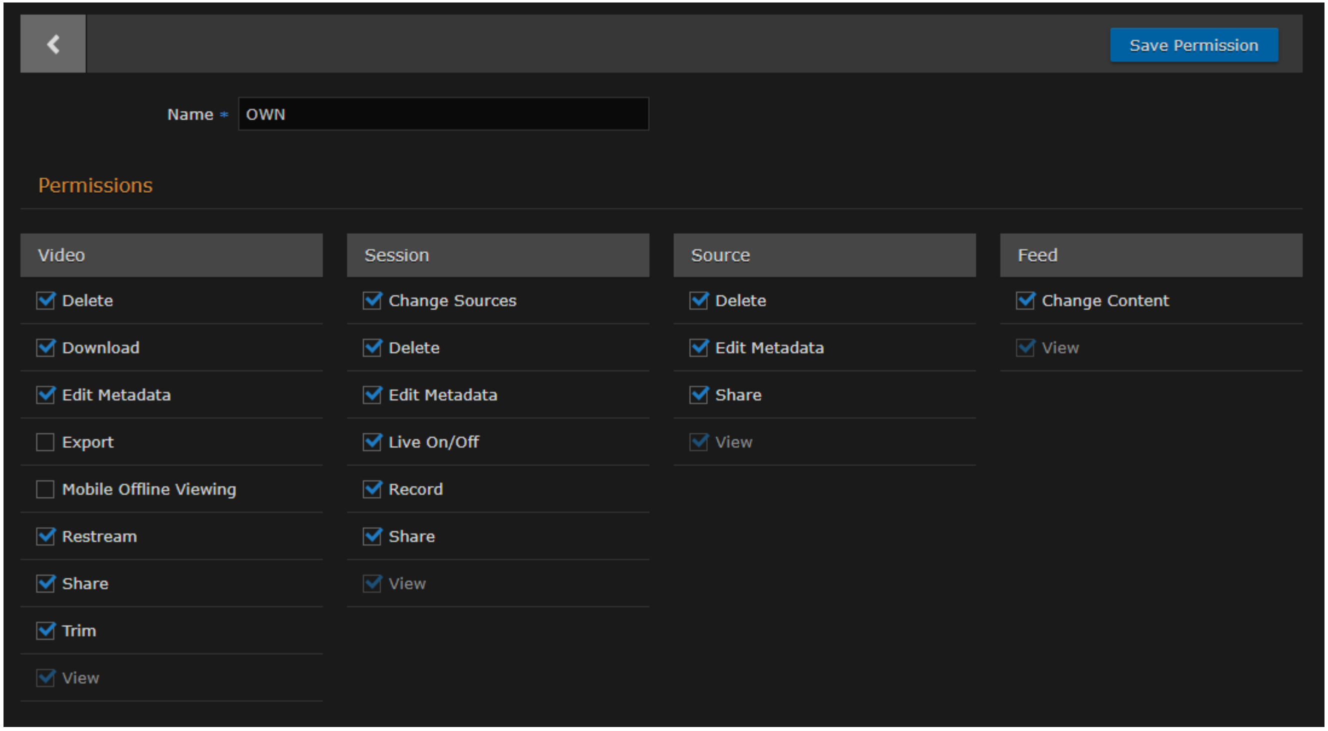
| Share Permission |
|---|
| □ OWN (Default) |
| □ EDIT |
| □ WATCH |
| □ MOBILEDOWNLOAD |

2. To create new a share permission, click the ⊕ icon.
3. On the Add Permission dialog, type in a name for the share permission and click **Add Permission**.



Name * SharePermission - 6/22/2018, 11:50 AM

4. On the Share Permissions Information pane, check the permissions to assign to the share permission.



Name * OWN

Permissions

| Video | Session | Source | Feed |
|---|---|---|---|
| ☑ Delete | ☑ Change Sources | ☑ Delete | ☑ Change Content |
| ☑ Download | ☑ Delete | ☑ Edit Metadata | ☑ View |
| ☑ Edit Metadata | ☑ Edit Metadata | ☑ Share | |
| ☐ Export | ☑ Live On/Off | ☑ View | |
| ☐ Mobile Offline Viewing | ☑ Record | | |
| ☑ Restream | ☑ Share | | |
| ☑ Share | ☑ View | | |
| ☑ Trim | | | |
| ☑ View | | | |

5. Click **Save Permissions**.
6. Click the ‹ icon to return to the Share Permissions list. This share permission is now available to users when sharing 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.

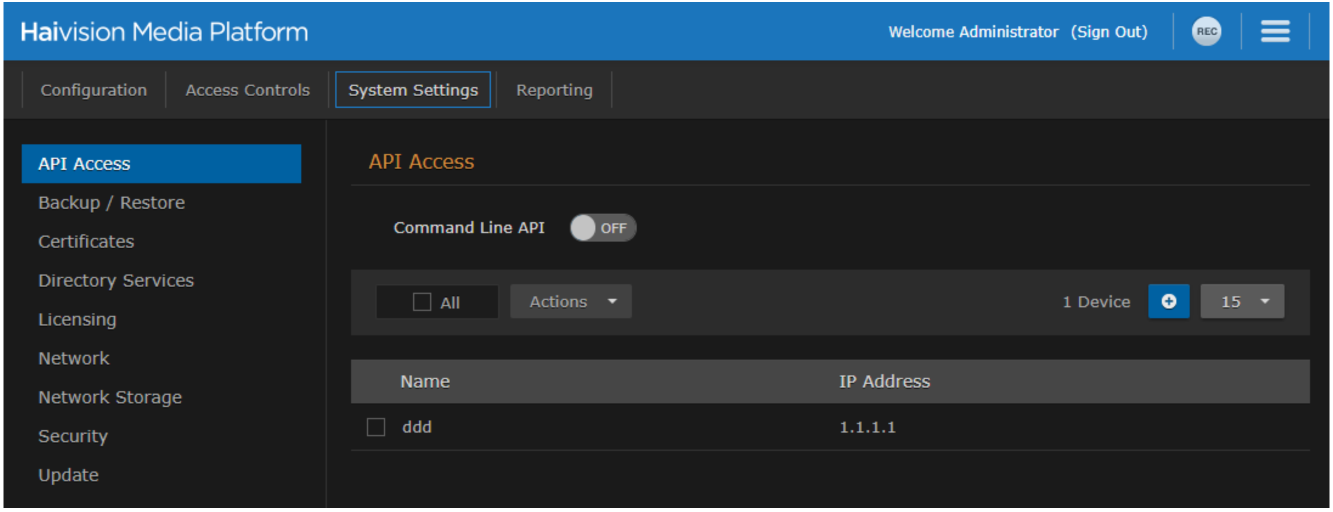
**Topics Discussed**

## Activating Command Line API Access

In order to use the Command Line API, you need to activate Command Line API access on Haivision Media Platform and add the client devices to the list of authorized devices.

To activate Command Line API access on HMP:

1. To navigate the Administration screen, click the ☰ icon on the banner and select **Administration** from the navigation drop-down menu.
2. On the Administration screen, 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).



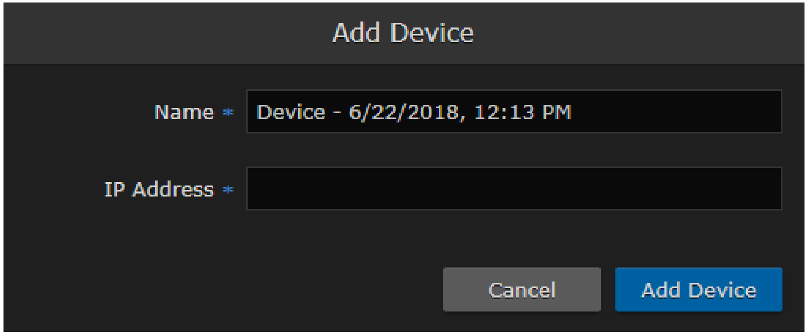
Command Line API OFF

| Name | IP Address |
|---|---|
| ddd | 1.1.1.1 |

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

> **Note**
>
> Toggling this button activates all devices in the list.

4. To add a device to the list, click the ⊕ icon.
5. On the Add Device dialog, enter a unique name that identifies this device.



Add Device

Name * Device - 6/22/2018, 12:13 PM

IP Address *

6. Enter the IP address of the device that will be accessing the Command Line API.
7. Click **Add Device**. The new device will be added to the list of authorized devices.

> **Note**
>
> Further changes to the list of authorized devices will be applied automatically. You do not need to restart HMP.

## Backing Up and Restoring HMP

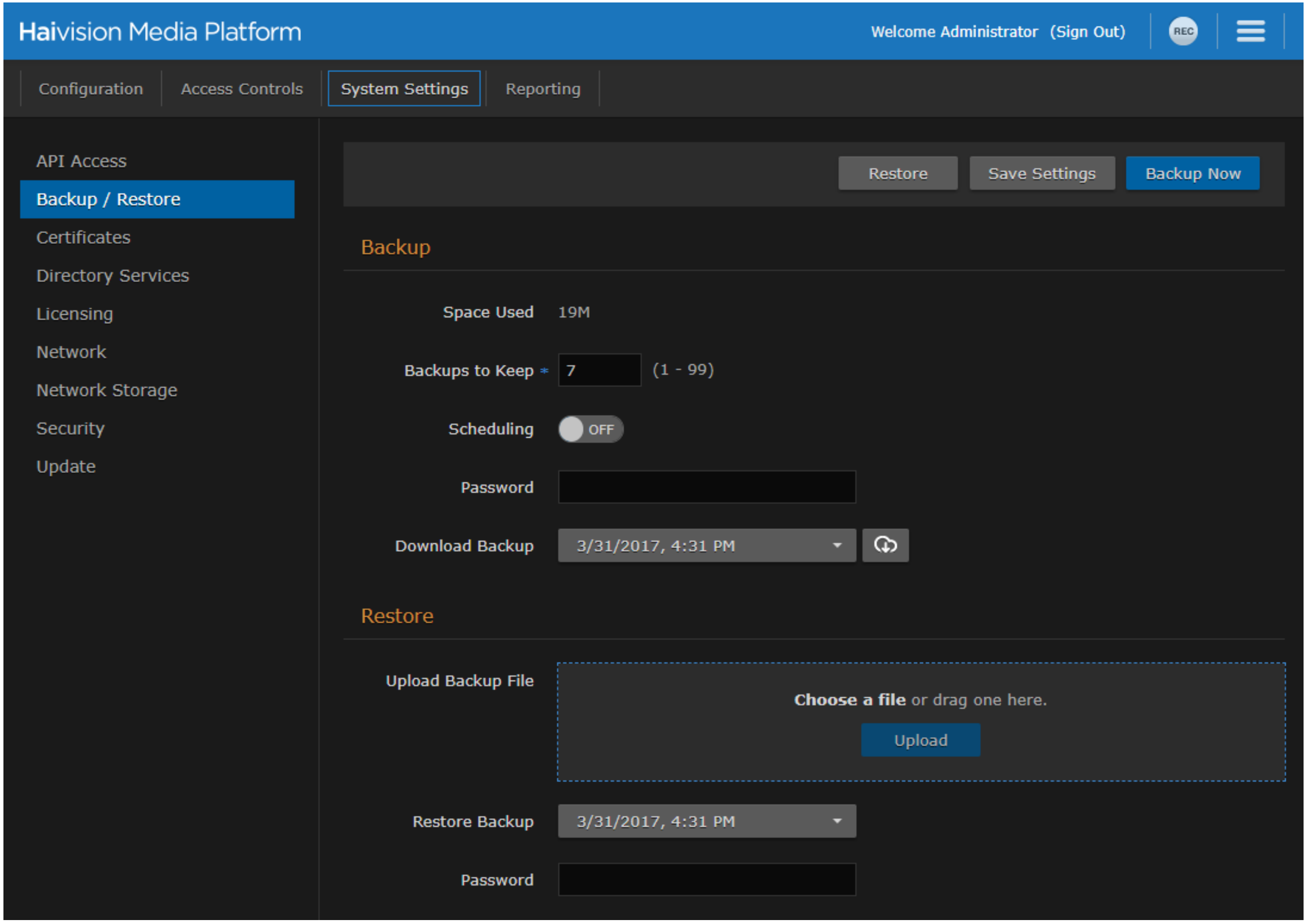
From the Backup/Restore pane, you can back up your Haivision Media Platform system configuration and permission information, either to a network storage location or your local server, and restore from that location. The backup includes local configuration such as sources and sessions (but not LDAP user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

> **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, make sure NFS is set to On and configured. See Managing Network Storage. Otherwise when NFS is Off or not available, backups are written to the local server.

To configure and schedule backups:

1. On the Administration screen, 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.



Space Used 19M

Backups to Keep * 7 (1 - 99)

Scheduling OFF

Password

Download Backup 3/31/2017, 4:31 PM

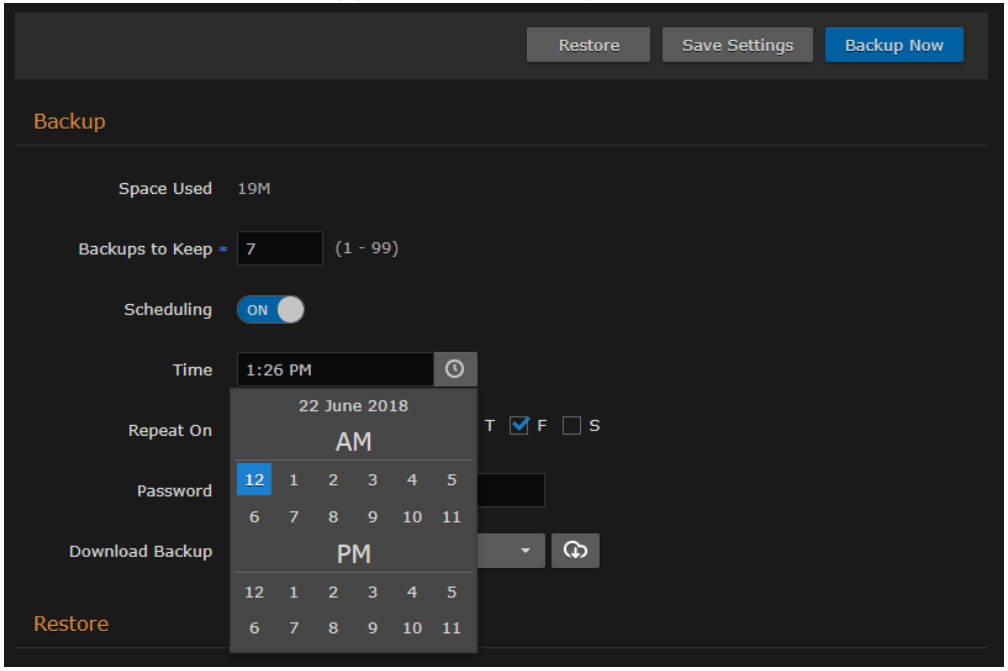
Upload Backup File

Restore Backup 3/31/2017, 4:31 PM

Password

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

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



Space Used 19M

Backups to Keep * 7 (1 - 99)

Scheduling ON

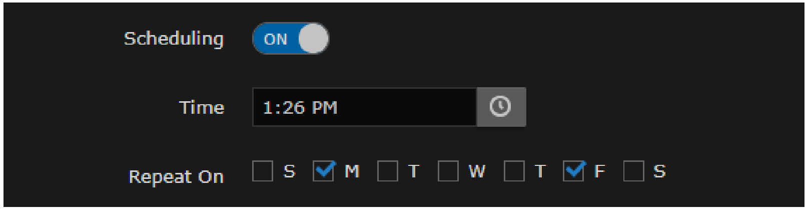
Time 1:26 PM

Repeat On T ☑ F □ S

Password

Download Backup

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



Scheduling ON

Time 1:26 PM

Repeat On □ S ☑ M □ T □ W □ T ☑ F □ S

5. **Important**

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

6. Click **Save Settings**.

### Topics Discussed

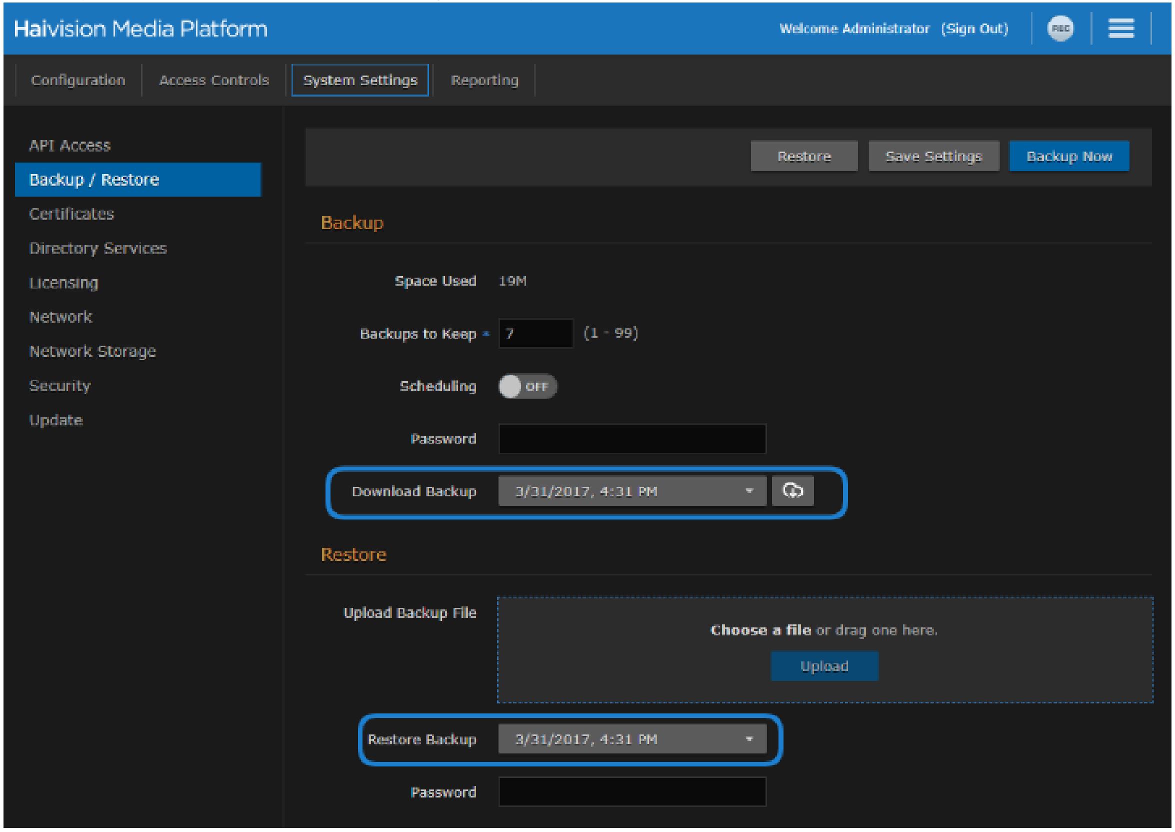
- Backing Up HMP
- Uploading Downloaded Files
- Restore to a Previous Configuration
- Backup/Restore Settings

## Backing Up HMP

To back up HMP:

1. To back up your system immediately, click **Backup Now**.
   HMP will back up your local configuration and permissioning information and add the new file to the Download Backup and Restore Backup drop-down lists (available once there has been a

backup, as shown in the following example).



Backup

Space Used 19M

Backups to Keep * 7 (1 - 99)

Scheduling OFF

Password

Download Backup 3/31/2017, 4:31 PM

Restore

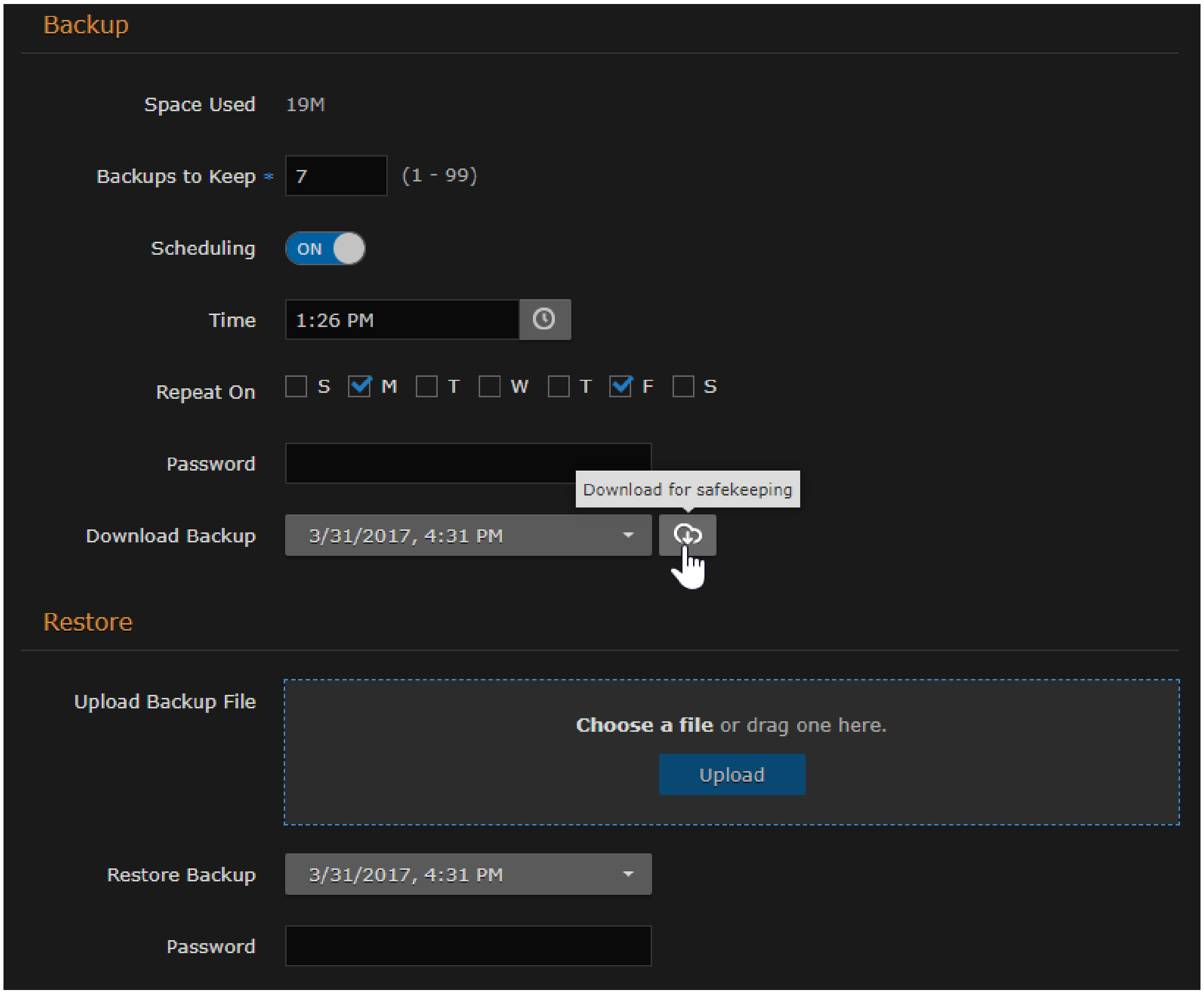
Upload Backup File

Choose a file or drag one here.

Restore Backup 3/31/2017, 4:31 PM

Password

2. To download a backup file (for example, to your local computer for safekeeping), select the file from the Download Backup list, click the ☁ icon, and select the location for the file in the Save File dialog.



Backup

Space Used 19M

Backups to Keep * 7 (1 - 99)

Scheduling ON

Time 1:26 PM

Repeat On □ S ☑ M □ T □ W □ T ☑ F □ S

Password

Download Backup 3/31/2017, 4:31 PM

Restore

Upload Backup File

**Choose a file** or drag one here.

Restore Backup 3/31/2017, 4:31 PM

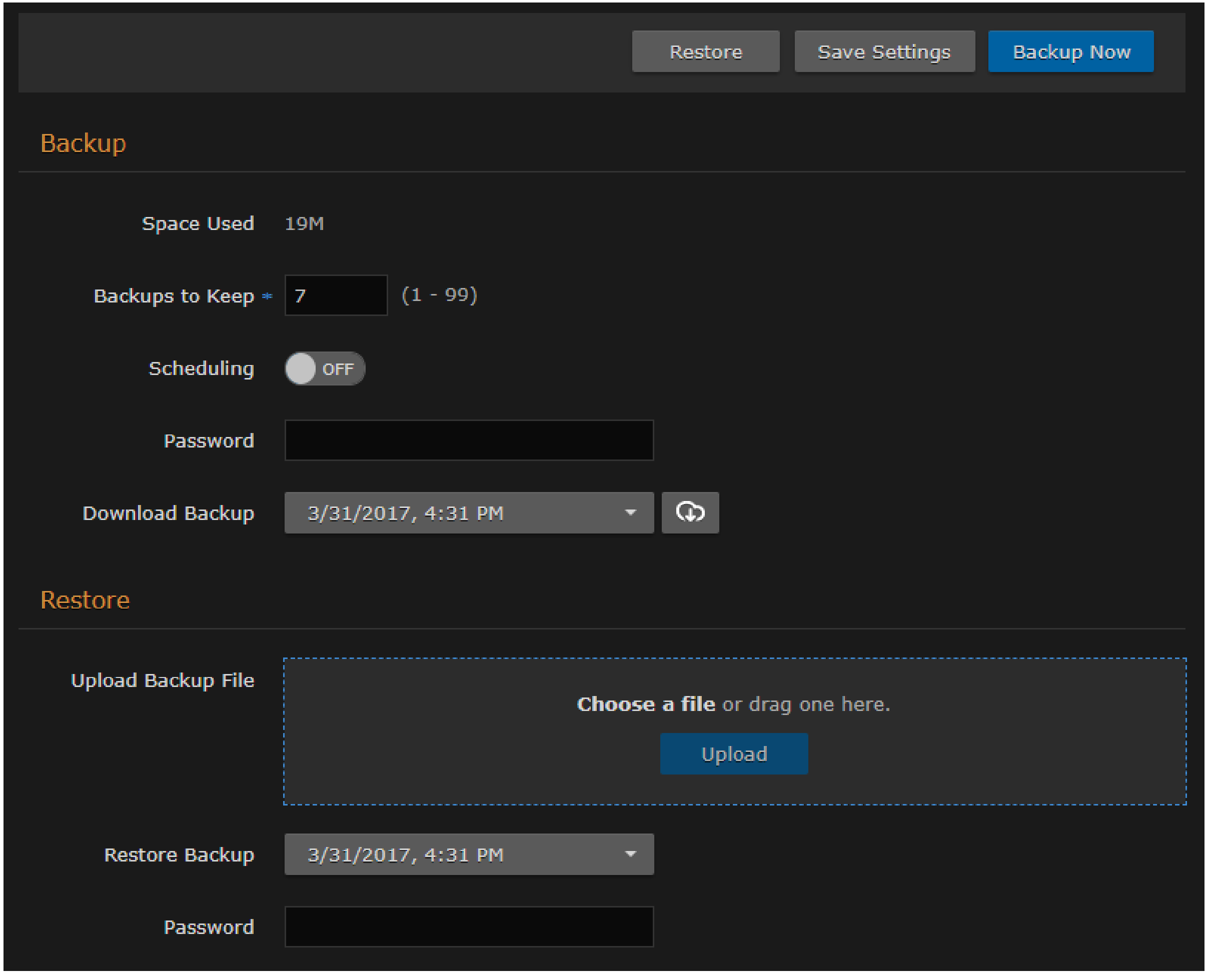
Password

The generated backup file is a .zip file with the syntax shown in the following example: “backup-1467139422.zip”.

## Uploading Downloaded Files

To upload a previously downloaded file:

1. On the Backup/Restore pane, drag a file to the drop area or click **Choose a file**, and then select a file to upload in the Open File dialog.
   The backup file must be a .zip file with the syntax shown in the following example: "backup-1467139422.zip".



Backup

Space Used 19M

Backups to Keep * 7 (1 - 99)

Scheduling OFF

Password

Download Backup 3/31/2017, 4:31 PM

Restore

Upload Backup File

**Choose a file** or drag one here.

Restore Backup 3/31/2017, 4:31 PM

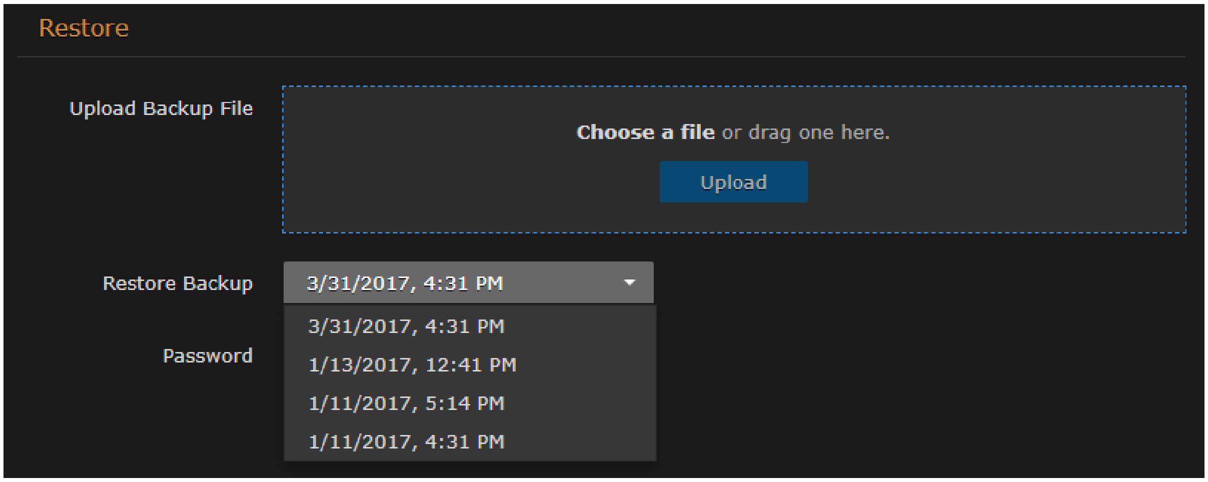
Password

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.



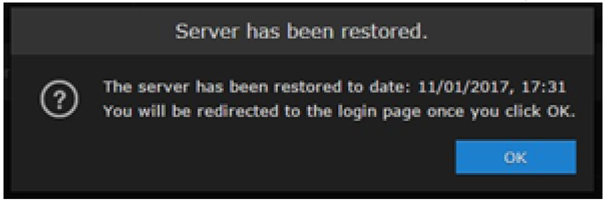
Restore

Upload Backup File: **Choose a file** or drag one here.

Restore Backup: 3/31/2017, 4:31 PM

Password

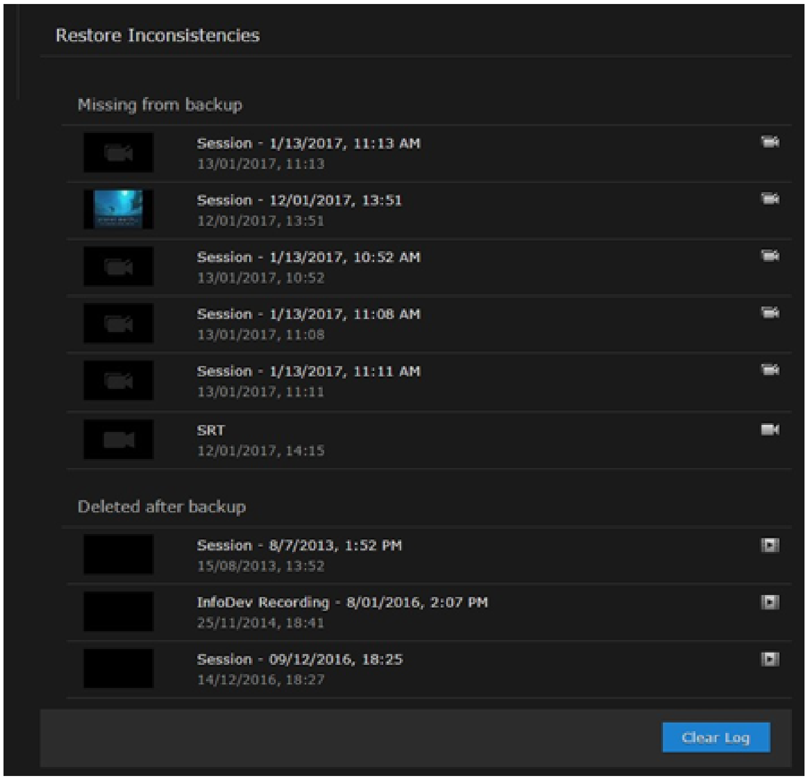
2. If the file is password-protected, type in the password in the Password field.
3. Click **Restore** and then click **Confirm**.
4. On the Server Has Been Restored dialog, click **OK** to proceed.



Server has been restored.

The server has been restored to date: 11/01/2017, 17:31
You will be redirected to the login page once you click OK.

5. Wait until the update is complete and HMP restarts. Once the appliance has restarted, the browser will display the HMP Sign-in screen (depending on your Web browser and settings). If not, reload the Sign-in screen.
6. If any changes have been made to the HMP configuration, such as sources, sessions, or videos since the backup was made, the inconsistent items will be listed under Restore Inconsistencies.



Restore Inconsistencies

Missing from backup

Session - 1/13/2017, 11:13 AM
13/01/2017, 11:13

Session - 12/01/2017, 13:51
12/01/2017, 13:51

Session - 1/13/2017, 10:52 AM
13/01/2017, 10:52

Session - 1/13/2017, 11:08 AM
13/01/2017, 11:08

Session - 1/13/2017, 11:11 AM
13/01/2017, 11:11

SRT
12/01/2017, 14:15

Deleted after backup

Session - 8/7/2013, 1:52 PM
15/08/2013, 13:52

InfoDev Recording - 8/01/2016, 2:07 PM
25/11/2014, 18:41

Session - 09/12/2016, 18:25
14/12/2016, 18:27

7. 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.
8. 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

### Backup

| Setting | Description |
|---|---|
| Space Used | The amount of disk/file spaced used for backups. |
| Backups to Keep | The number of backups to keep. When the maximum number is reached, HMP will delete the oldest file to make room for the newest. 1-99 |
| Scheduling | To schedule backups, toggle the Scheduling button to On. The Time and Repeat On fields then become available. |
| Time | (Scheduling must be On) Type in or use the calendar to adjust the start date and time. |
| Repeat On | (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, type in a password that will be required to restore the backup. |
| Download Backup | (Available once there has been a backup) Select a backup file to download from the drop-down list of download dates. |
| ⬇ | (Available once there has been a backup) Click to download the selected backup file. |

Backup Restore

### Restore

| Setting | 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, type in 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).

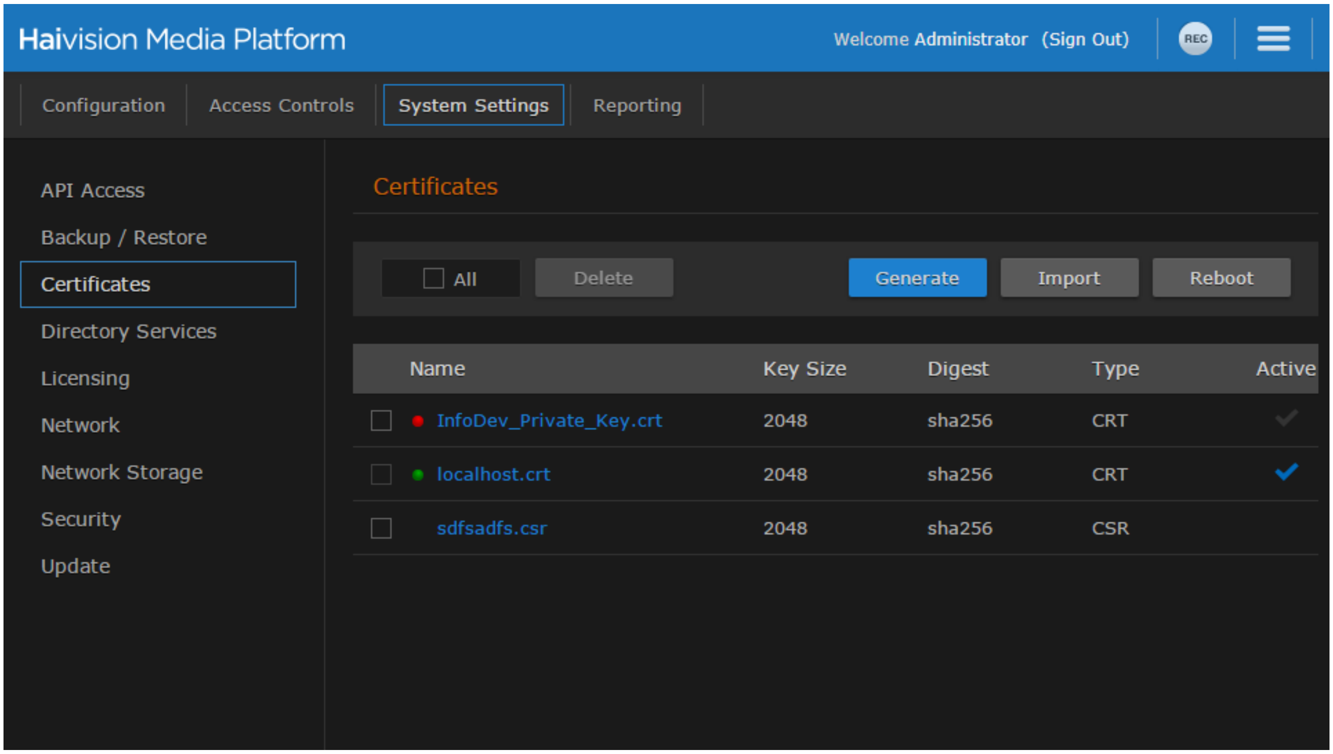
**Topics Discussed**

- Generating a Certificate Signing Request (CSR)
- Importing and Activating a Certificate (CRT)
- Generating a Private Key
- Importing a Private Key
- Certificate Settings

## Generating a Certificate Signing Request (CSR)

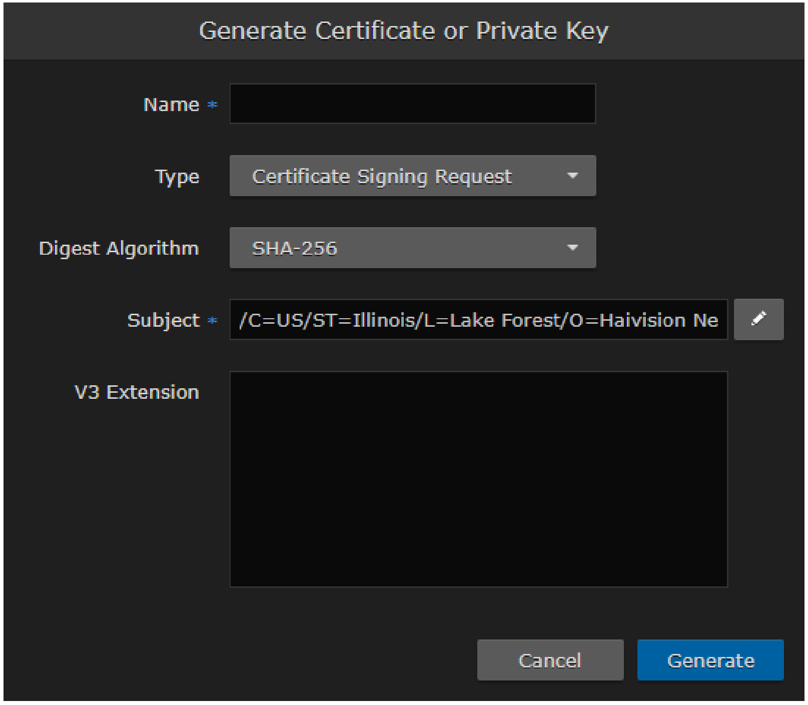
To generate a Certificate Signing Request (CSR):

1. On the Administration screen, 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 blue check.



| | Name | Key Size | Digest | Type | Active |
|---|---|---|---|---|---|
| ☐ | ● InfoDev_Private_Key.crt | 2048 | sha256 | CRT | ✓ |
| ☐ | ● localhost.crt | 2048 | sha256 | CRT | ✓ |
| ☐ | sdfsadfs.csr | 2048 | sha256 | CSR | |

2. Click **Generate**.
3. On the Generate Certificate or Private Key dialog, type in a name for the certificate.



Generate Certificate or Private Key

Name *

Type: Certificate Signing Request

Digest Algorithm: SHA-256

Subject *: /C=US/ST=Illinois/L=Lake Forest/O=Haivision Ne

V3 Extension

4. Make sure the Type is Certificate Signing Request and fill in the remaining fields. See **Certificate Settings**.
5. For the subject, type in information about the device that the Identity Certificate represents. For more information, see the "Subject" entry in **Certificate Settings**.
6. Click **Generate**.

> **Note**
>
> The generated CSR file needs to be sent to a Certification Authority to be signed. The CSR content can be viewed by clicking on the CSR name in the list; its content will be displayed in a new window where it can be copied.You can import the signed certificate back later by clicking the Import button.

7.

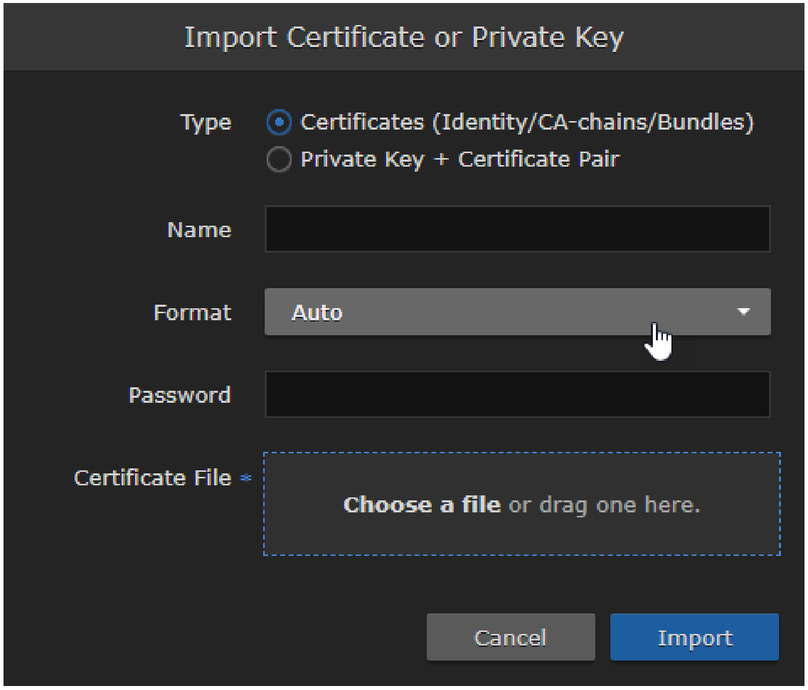
> **Tip**
>
> Keep in mind that there is a difference between importing a new certificate (that was generated externally) and importing a newly signed certificate whose request was previously generated on HMP and exported for signing.

## Importing and Activating a Certificate (CRT)

To import and activate a Certificate (CRT):

1. On the Certificates pane, click **Import**.

2. On the Generate Certificate or Private Key dialog, keep the default Type: Certificates (Identity/CA-chains/Bundles).



Import Certificate or Private Key

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

Name

Format Auto

Password

Certificate File *

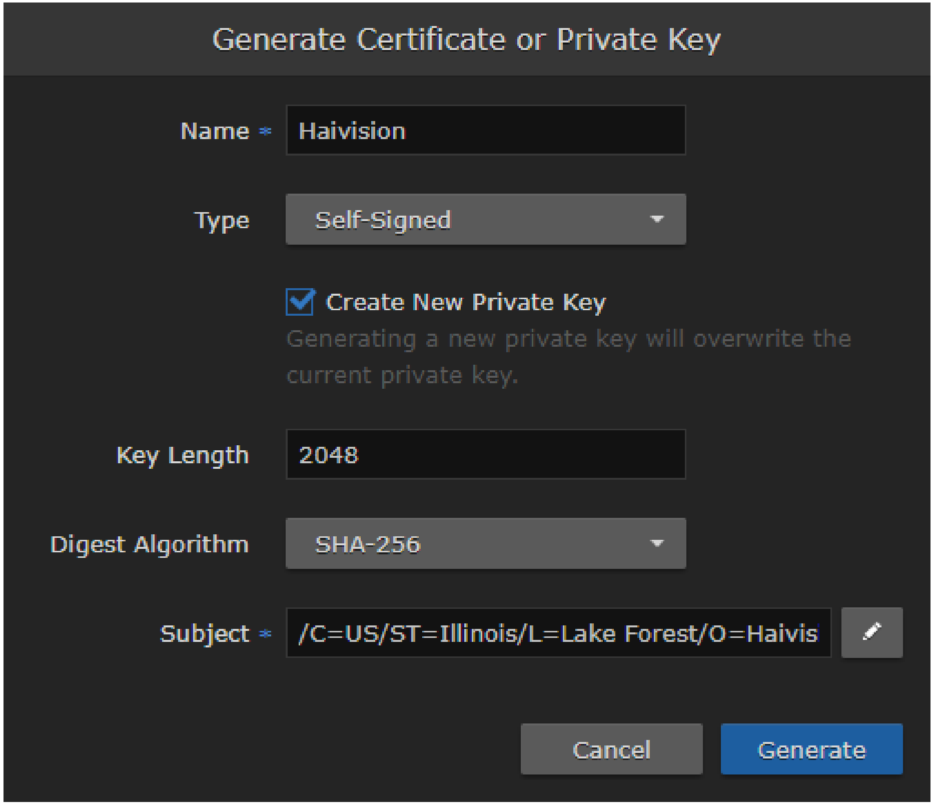
**Choose a file** or drag one here.

3. Type in the certificate name and fill in the remaining fields. See Certificate Settings.
4. If your certificate is encrypted, type in the password.
5. Drag a CA-signed certificate (CRT) to the drop area or click **Choose a file to choose** and select the certificate (returned from the certificate request generated in the previous section).
6. Click **Import**. On the Certificates pane, the newly imported certificate will be added to the list and should have a green status LED. Click in the Active column to activate the certificate.
7. Click **Reboot** if you have changed the active certificate.

## 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, type in 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

5. Fill in the remaining fields. See Certificate Settings.
6. Click **Generate**.

   **Caution**

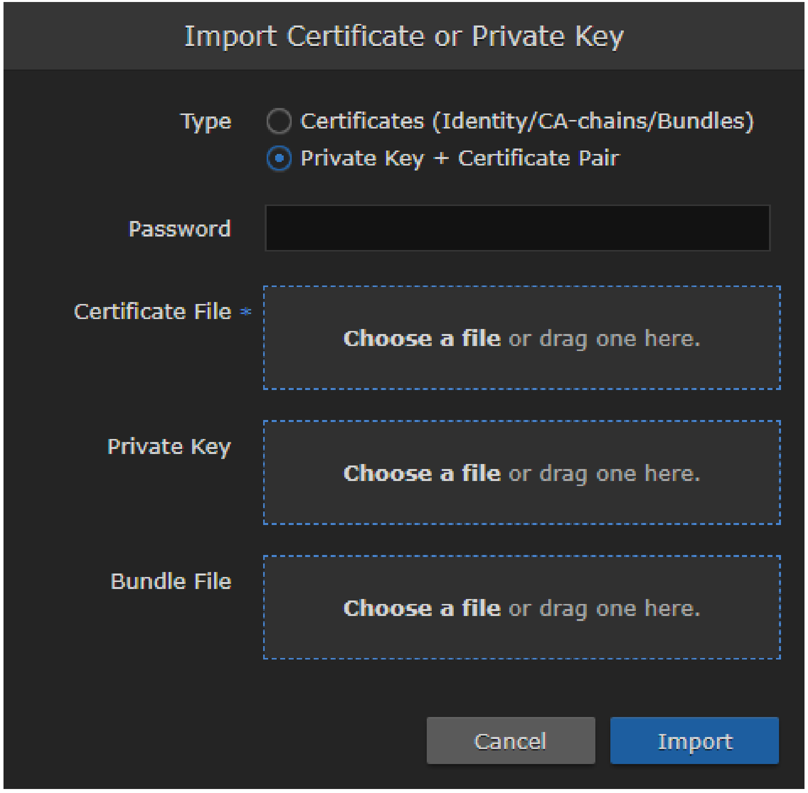
   Clicking Generate will overwrite the current private key and render unusable any certificates based on that key.

   The new certificate is added to the Certificates list, and becomes the active certificate.
7. Click **Reboot**.

## 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

Choose a file or drag one here.
Choose a file or drag one here.
Choose a file or drag one here.
Cancel
Import

3. Type in 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 will be added to the list.
6. Click **Reboot**.

## Certificate 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.

Generate Certificate or Private Key Import Certificate

### Generate Certificate or Private Key

| Setting | Description |
|---|---|
| Name | Type in a unique name under which the certificate will be stored on HMP as well as listed on the Certificate pane |
| Type | Select the Signature Type:<br>• Self-signed: The certificate will be generated and signed by the system, and the name will be added to the list of Identity Certificates.<br>• Certificate Signing Request: A request will be generated, and its name will be added to the list of Identity Certificates. The request will be 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):<br>• SHA-256<br>• SHA-384<br>• SHA-512 |
| Subject | The Subject identifies the device being secured, in this case, HMP. Type in the subject in the form: "/C=.../ST=.../L=.../O=.../OU=.../CN=..." where the most common attributes are:<br>• /C Two Letter Country Name<br>• /ST State or Province Name<br>• /L Locality Name<br>• /O Organization Name<br>• /OU Organizational Unit Name<br>• /CN Common Name<br>**Tip**<br>For successful authentication, the Common Name in the certificate should be the IP address (by default) or domain name of the device. |

| Setting | Description |
|---|---|
| V3 Extension | V3 extensions allow more configuration options to be inserted in the Code Signing Request, such as alternative subject names and usage restrictions to certificates.<br>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:<br>`[ req ]`<br>`req_extensions = v3_req`<br>`[ v3_req ]`<br>`# Extensions to add to a certificate request`<br>`subjectAltName = @alt_names`<br>`[ alt_names ]`<br>`DNS.1 = server1.example.com`<br>`DNS.2 = mail.example.com`<br>`DNS.3 = www.example.com`<br>`DNS.4 = www.sub.example.com`<br>`DNS.5 = mx.example.com`<br>`DNS.6 = support.example.com` |

Generate Certificate or Private Key    Import Certificate

### Import Certificate

| Setting | Description |
|---|---|
| Type | Select the certificate Type:<br>• Certificates: (Identify/CA-chains/Bundles)<br>• Private Key + Certificate Pair |
| Name | Name of the certificate. |
| Format | Select the file format for the Certificate (the formats differ in the way the file is encrypted):<br>• Auto: detected from the file extension<br>• der: Distinguish Encoding Rules<br>• pkcs #7<br>• 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

**Important**

If Haivision Media Platform is connected to an LDAP or Active Directory server, the Users and Groups lists will be 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.**

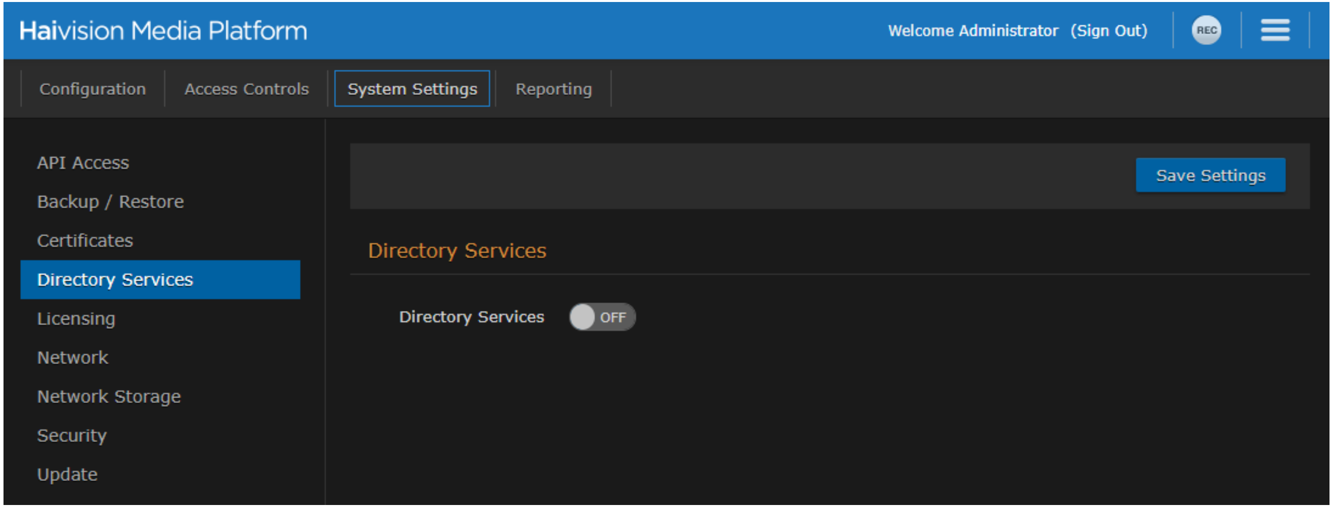
**Topics Discussed**

- 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

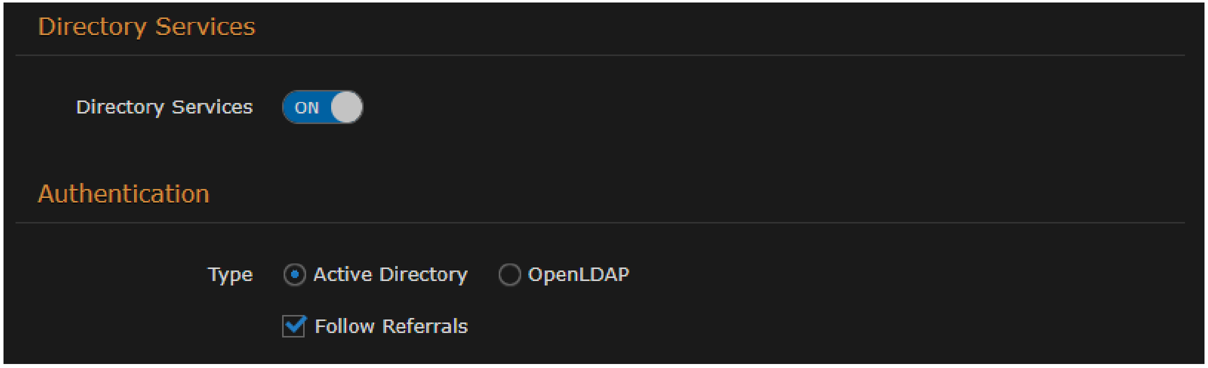
To connect HMP to a Directory Server:

1. On the Administration screen, click **System Settings** on the toolbar and then click **Directory Services** on the sidebar.
   The Directory Services pane opens.



Directory Services OFF

2. 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.



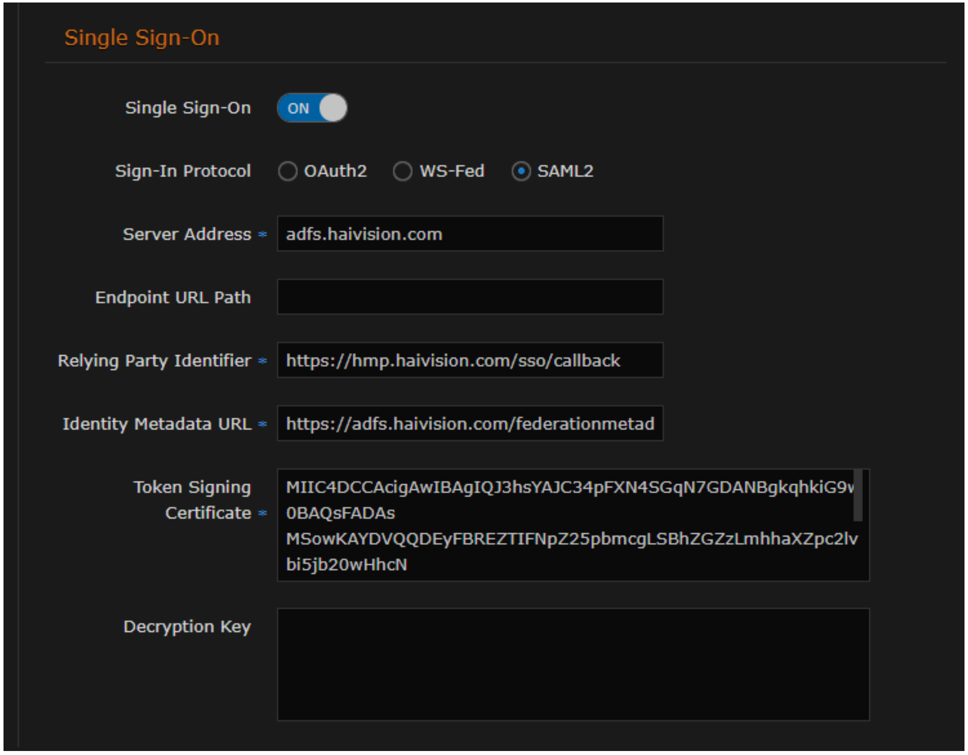
Directory Services ON

Type ● Active Directory ○ OpenLDAP

☑ Follow Referrals

3. Under Authentication, select type of LDAP implementation for your system, either:
   - Active Directory: An implementation of LDAP directory services by Microsoft.
   - Open LDAP: An open source implementation of LDAP directory services.
4. For the server Connection, Query, and Data Mapping settings, enter or select the new value(s) in the appropriate field(s). See **Directory Service Settings**.

5. To configure Single Sign-On (SSO), enter or select the new value(s) in the appropriate field(s). See Integrating HMP with Single Sign-On (SSO) Environments.



Single Sign-On

Single Sign-On: ON

Sign-In Protocol: ○ OAuth2 ○ WS-Fed ● SAML2

Server Address *: adfs.haivision.com

Endpoint URL Path:

Relying Party Identifier *: https://hmp.haivision.com/sso/callback

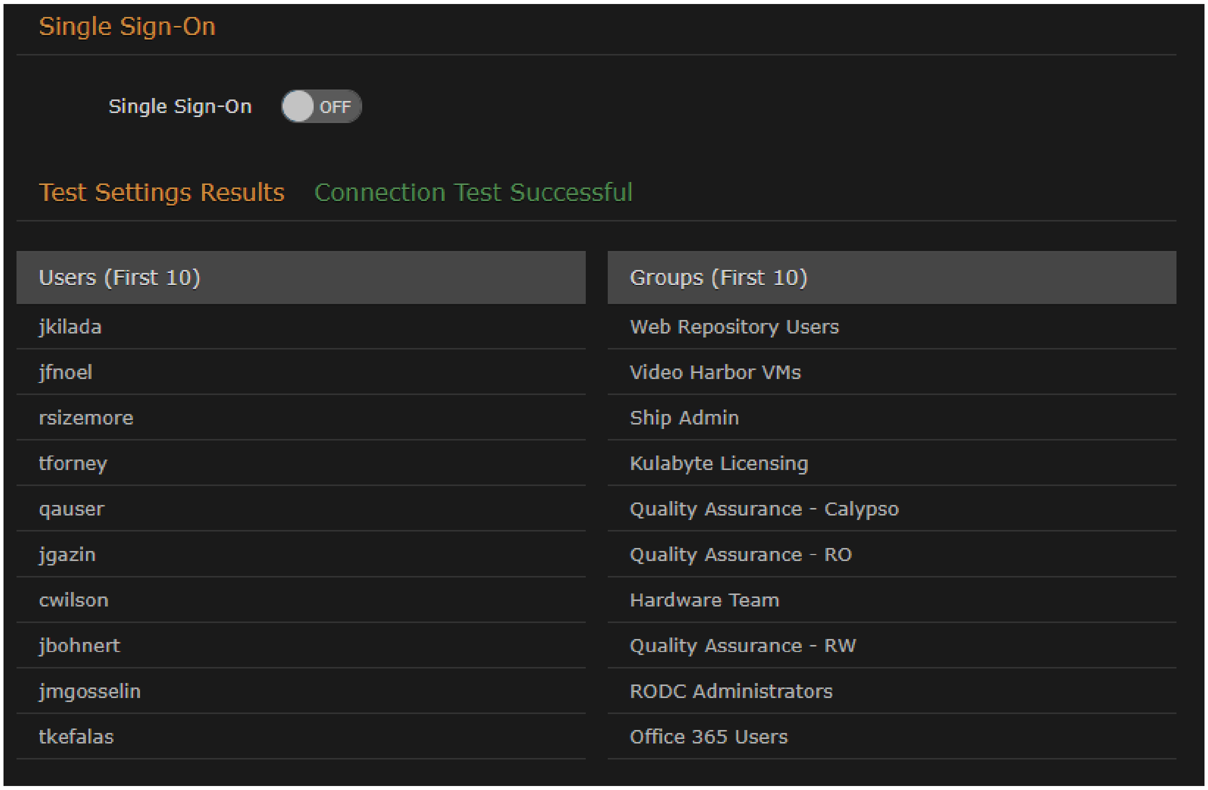
Identity Metadata URL *: https://adfs.haivision.com/federationmetad

Token Signing Certificate *:
MIIC4DCCAcigAwIBAgIQJ3hsYAJC34pFXN4SGqN7GDANBgkqhkiG9w
0BAQsFADAs
MSowKAYDVQQDEyFBREZTIFNpZ25pbmcgLSBhZGZzLmhhaXZpc2lv
bi5jb20wHhcN

Decryption Key:

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

> **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 will be displayed (as shown in the following example).



Test Settings Results Connection Test Successful

| Users (First 10) | Groups (First 10) |
|---|---|
| jkilada | Web Repository Users |
| jfnoel | Video Harbor VMs |
| rsizemore | Ship Admin |
| tforney | Kulabyte Licensing |
| qauser | Quality Assurance - Calypso |
| jgazin | Quality Assurance - RO |
| cwilson | Hardware Team |
| jbohnert | Quality Assurance - RW |
| jmgosselin | RODC Administrators |
| tkefalas | Office 365 Users |

7. Click **Save Settings** to save the connection.
   The Users and Groups lists will now be 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**.
   The LDAP or Active Directory information will be removed from HMP, and the Users and Groups panes will 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

### Authentication

| Setting | Default | Description/Values |
|---|---|---|
| Type | Active Directory | Select your authentication server type:<br>• Active Directory<br>• OpenLDAP |
| Follow Referrals | Enabled | Referral following is enabled when this checkbox is checked (default).<br>• 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.<br>• When disabled, the LDAP client does not connect to any other servers besides the one specified by the Connection settings.<br>**Tip**<br>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. |

Authentication Connection Query Data Mapping Single Sign-On

### Connection

| Setting | Default | Description/Values |
|---|---|---|
| IP Address | n/a | 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. |

| Setting | Default | Description/Values |
|---|---|---|
| Connection | Basic | Select the encryption protocol:<br>• Basic: Unencrypted connection<br>• SSL: Secure Socket Layer (recommended) |
| Username | n/a | 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 | n/a | The password that corresponds with the user name provided for the Username field. |
| Sync Interval | 60 minutes | The directory server sync interval. |

Authentication Connection **Query** Data Mapping Single Sign-On

### Query

| Setting | Default | Description/Values |
|---|---|---|
| Base DN | n/a | The Base DN (Distinguished Name) used by your authentication system. This setting should be provided by your AD/LDAP administrator. For example: `ou=staff,dc=haivision,dc=com`<br>**Note**<br>Spaces are not allowed unless they are part of the path.<br>**Important**<br>If the Base DN is wrong, HMP will not be able to access the groups. When the connection test succeeds, you will see a list of the first 10 users and groups (see example in Connecting to a Directory Server). |
| User Context | n/a | 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: `ou=people,dc=haivision,dc=com`<br>**Important**<br>If the User Context is wrong, users will not be able to sign in correctly. For example, they may only have the anonymous privileges or even a blank screen.<br>**Note**<br>In order 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). |
| Group Context | n/a | **Note**<br>See previous Note to input multiple Group Contexts. |

| Setting | Default | Description/Values |
|---|---|---|
| User Attribute | sAMAccount Name | The user attribute your directory system uses. OpenLDAP systems normally use “ `cn` ” or “ `uid` ”, while Active Directory systems normally use “ `sAMAccountName` ”. |
| Member Attribute | memberOf | The member attribute your directory system uses. OpenLDAP systems normally use “ `member` ” or “ `memberUid` ”, while Active Directory systems normally use “ `memberOf` ”. |
| Group Object Class | (\|(objectClass= group)<br>(objectClass= groupOfNames )) | Object class query for groups. The default will work with almost all directory servers |
| User Object Class | (objectClass= person) | Object class query for users. The default will work 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 will be attempted. The default on most directory servers is 1000. |

Authentication Connection Query **Data Mapping** Single Sign-On

### Data Mapping

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

Authentication Connection Query Data Mapping **Single Sign-On**

### 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. Once 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.

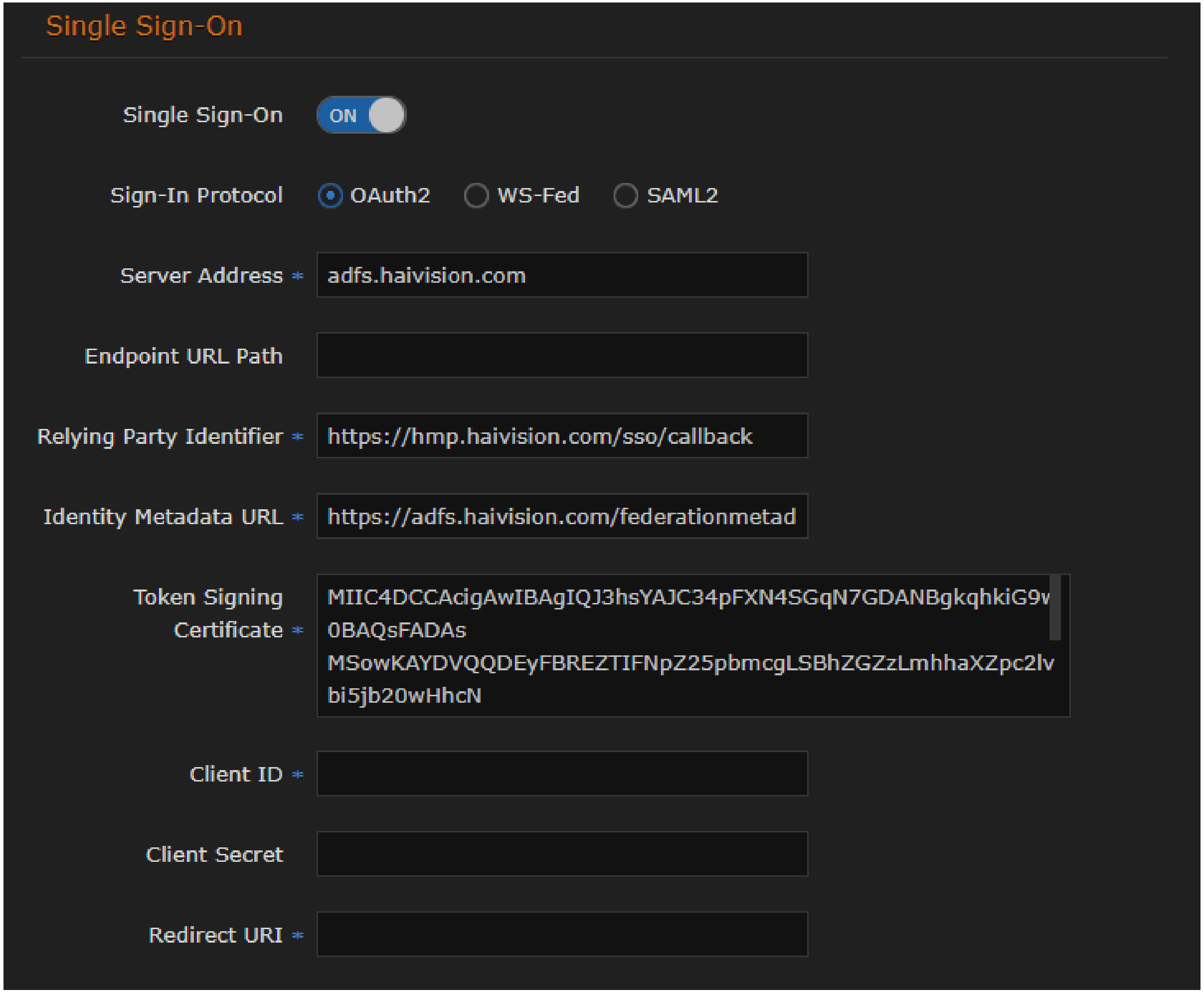
- WS-Fed and SAML2 work for Windows Server 2008+ / AD FS 2.0+ and Azure,
- OAuth2 works for Windows Server 2012 R2 / AD FS 3.0+ and Azure.

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**.



Single Sign-On

| | |
|---|---|
| Single Sign-On | ON |
| Sign-In Protocol | ● OAuth2 ○ WS-Fed ○ SAML2 |
| Server Address * | adfs.haivision.com |
| Endpoint URL Path | |
| Relying Party Identifier * | https://hmp.haivision.com/sso/callback |
| Identity Metadata URL * | https://adfs.haivision.com/federationmetad |
| Token Signing Certificate * | MIIC4DCCAcigAwIBAgIQJ3hsYAJC34pFXN4SGqN7GDANBgkqhkiG9w<br>0BAQsFADAs<br>MSowKAYDVQQDEyFBREZTIFNpZ25pbmcgLSBhZGZzLmhhaXZpc2lv<br>bi5jb20wHhcN |
| Client ID * | |
| Client Secret | |
| Redirect URI * | |

3.

> **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.

4. Enter value(s) in the remaining field(s). 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 should be sufficient. | For Azure AD, it's 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: https://login.microsoftonline.com/514a94b9-6a5b-4f0b-96aa-63dced118308 |
| 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. When the Sign-In Protocol is OAuth2, the Endpoint URL Path should not include the "authorize" or "token" portions of the URL, because HMP adds these automatically. | If this is empty, HMP assumes that the default AD FS endpoint should be used for the chosen Sign-In Protocol<br>• For OAuth2, this is `/adfs/oauth2`<br>• For WS-Fed or SAML2, this is `/adfs/ls` | When using Azure AD, set this to the part of the sign-on endpoint that was omitted in the Server Address field.<br>• For OAuth2, that would be "/oauth2"<br>• For WS-Fed, "/`wsfed`"<br>• For SAML2, "/`saml2`" |
| 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. |

| Setting | Description | AD FS-specific | Azure AD-specific |
|---|---|---|---|
| Identity Metadata URL | When HMP's authentication service starts up, 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. | For AD FS, the value that should be entered will look something like:<br>✓ **Tip**<br>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. | ✓ **Tip**<br>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 will be labeled "FEDERATION METADATA DOCUMENT".<br>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). This URL should look something like this: https://login.microsoftonline.com/514a94b96a5b4f0b-96aa63dced118308/v2.0/.wellknown/openid-configuration |
| 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 will be 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 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. |

| Setting | Description | AD FS-specific | Azure AD-specific |
|---|---|---|---|
| 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 " `Get-AdfsClient` " PowerShell cmdlet. The `ClientId` and `RedirectUri` 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. |
| 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 https://calypso.local/sso/callback (replacing "calypso.local" 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. | | |

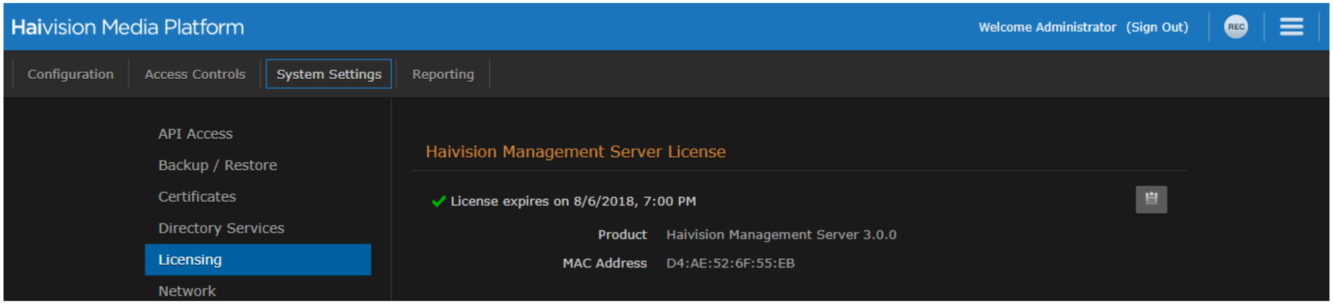
# Managing Licenses

This section provides instructions to update your Haivision Media Platform license from the Web interface.

> **Note**
>
> Any update (other than a maintenance release such as v2.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. On the Administration screen, click **System Settings** on the toolbar and then click **Licensing** on the sidebar.
   The License pane opens, showing the installed license, including its expiry date and license (Edition) features.



Haivision Management Server License

✓ License expires on 8/6/2018, 7:00 PM

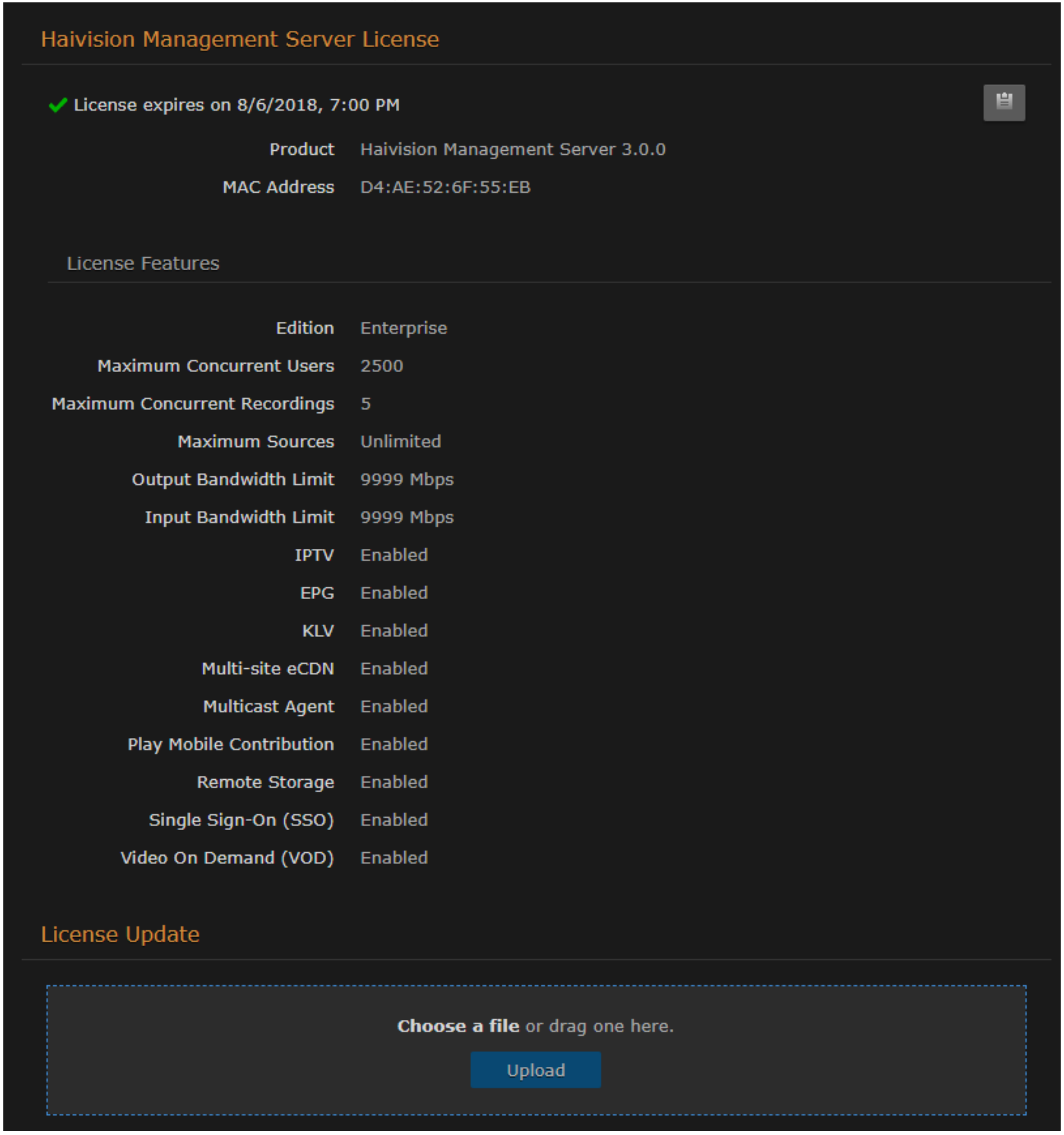
Product Haivision Management Server 3.0.0

MAC Address D4:AE:52:6F:55:EB

> **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.

2. Click 📋 to copy the current product details (product name, version and MAC address) to the clipboard.

3. Contact Haivision Technical Support with this information to request the license file.



Haivision Management Server License

✓ License expires on 8/6/2018, 7:00 PM

| | |
|---|---|
| Product | Haivision Management Server 3.0.0 |
| MAC Address | D4:AE:52:6F:55:EB |

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 | Enabled |
| Multi-site eCDN | Enabled |
| Multicast Agent | Enabled |
| Play Mobile Contribution | Enabled |
| Remote Storage | Enabled |
| Single Sign-On (SSO) | Enabled |
| Video On Demand (VOD) | Enabled |

License Update

**Choose a file** or drag one here.

4. Once you have the license file, drag it into the License Update drag area or click Choose a file.
5. Click **Upload** to upload the license to HMP.

## Configuring Network Settings

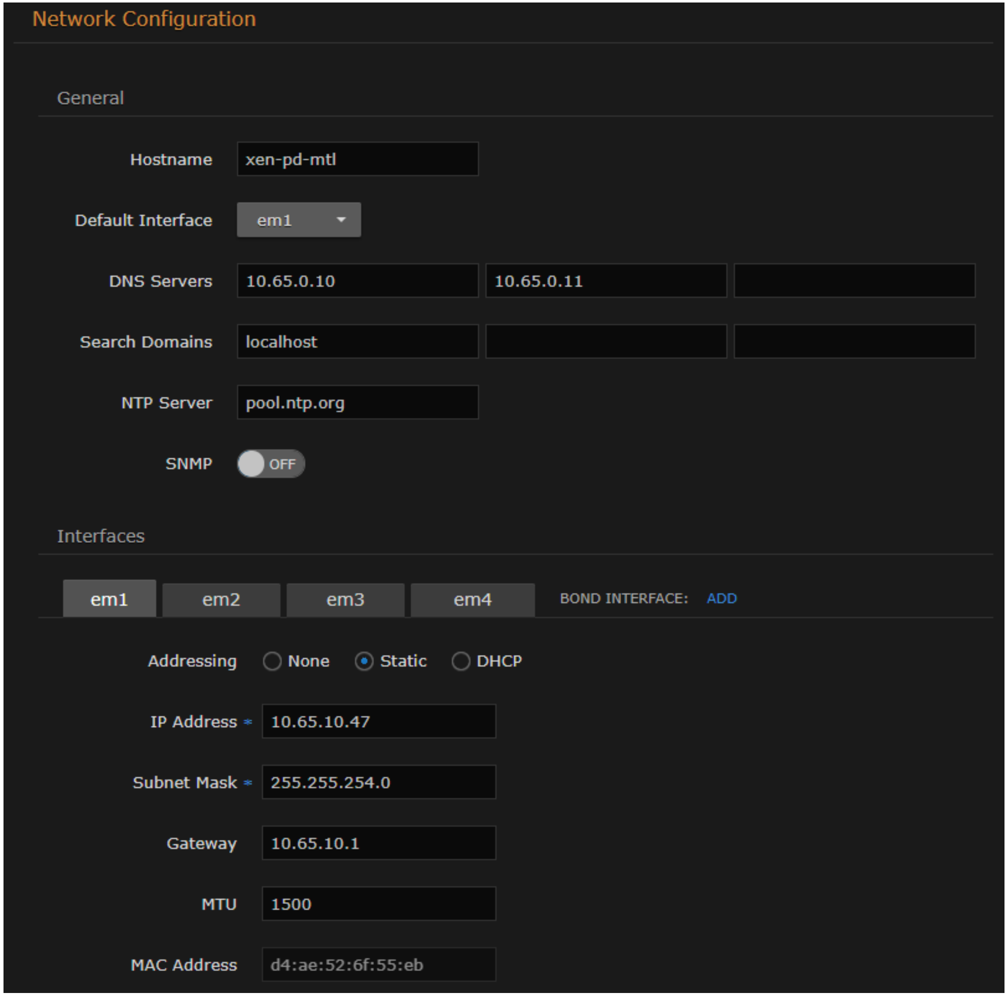
When setting up Haivision Media Platform, you will need to configure the network settings. This includes general settings such as specifying the server hostname, IP address, subnet mask, and DNS server(s), as well as advanced settings such as setting up multiple network interfaces, NIC bonding, link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

To configure the network settings:

1. On the Administration screen, click **System Settings** on the toolbar and then click **Network** on the sidebar.
   The Network Configuration pane opens.
2. Fill in the General section. For details, see Network Settings.
3. To enable SNMP alerts, toggle the SNMP button to **On**.
4. Under Interfaces, select the first interface, if not already selected.
5. **Note**

   When DHCP is enabled, HMP will get an IP Address from a DHCP server on the network to which it is connected. When it is disabled, you must manually enter the appliance's IP Address and Netmask.

6. Fill in the required fields. For details, see Network Settings.



Network Configuration

General

Hostname: xen-pd-mtl

Default Interface: em1

DNS Servers: 10.65.0.10 | 10.65.0.11 |

Search Domains: localhost | |

NTP Server: pool.ntp.org

SNMP: OFF

Interfaces

Addressing: ○ None ● Static ○ DHCP

IP Address *: 10.65.10.47

Subnet Mask *: 255.255.254.0

Gateway: 10.65.10.1

MTU: 1500

MAC Address: d4:ae:52:6f:55:eb

7. To configure multiple network interfaces, select the next interface (e.g., em2) and repeat the configuration.
8. 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.

9. To add one or more static routes, click **+Route** under Static Routes and fill in the fields.
10. Click **Save Settings**.
11. Click **Reboot** to restart the HMP server.

**Topics Discussed**

- Network Settings

## 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 | **Note**<br>Network Interface names for Ethernet interfaces may vary, such as eth0/eth1/... or em1/em2/.... "None" indicates that the default interface is not set. |
| DNS Servers | (Optional) The IPv4 address(es) of the Domain Name Server(s) to use. |
| Search Domains | (Optional) The search strings to use when attempting to resolve domain names. |
| NTP Server | (Optional) If Network Time Protocol (NTP) is enabled, enter the IP address of the NTP server. |
| SNMP | To enable SNMP (Simple Network Management Protocol) alerts for out-of-band monitoring, toggle this button to **On**.<br>This tells HMP to start the SNMP server, in order to query for OS information, such as CPU usage. SNMP alerts are typically used by IT administrators to monitor system health. |

| Setting | Description |
|---|---|
| Read-Only Community | (SNMP must be enabled) Type in 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) The SNMP server to send SNMP Traps to. This is an IPv4 or FQDN of an SNMP Trap server listening for traps via SNMP. For example: SNMP1.mycompany.com |

General Interfaces Static Routes

### Interfaces

| Setting | Description |
|---|---|
| eth0\|eth1\|eth2\|eth3 | **Note**<br>Network Interface names for Ethernet interfaces may vary, such as eth0/eth1/..., pNp1/pNp2/..., or em1/em2/.... |
| 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 will use a static or dynamic IP address: |
| IP Address | **Note**<br>If DHCP is disabled, you may enter an IP address in dotted-decimal format (xxx.xxx.xxx.xxx). |
| Subnet Mask | **Note**<br>If DHCP is disabled, you may enter a Network Mask in dotted-decimal format (e.g., 255.255.0.0). |
| Gateway | **Note**<br>If DHCP is disabled, you may enter a gateway address in dotted-decimal format. |
| 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. |
| 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). |

| Setting | Description |
|---|---|
| Bonding Mode | (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.<br>• Round Robin Sequential: Transmits packets in first available network interface (NIC) slave through the last. This mode provides load balancing and fault tolerance.<br>• 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<br>• 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.<br>• Broadcast – Fault Tolerance: Transmits network packets on all slave interfaces. This mode is least used (only for specific purpose) and provides only fault tolerance.<br>• 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.<br>• (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.<br>• (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 | **Note**<br>A static route cannot be created with a Subnet Mask of either 0.0.0.0 or 255.255.255.255. |

# Managing Network Storage

**Note**

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

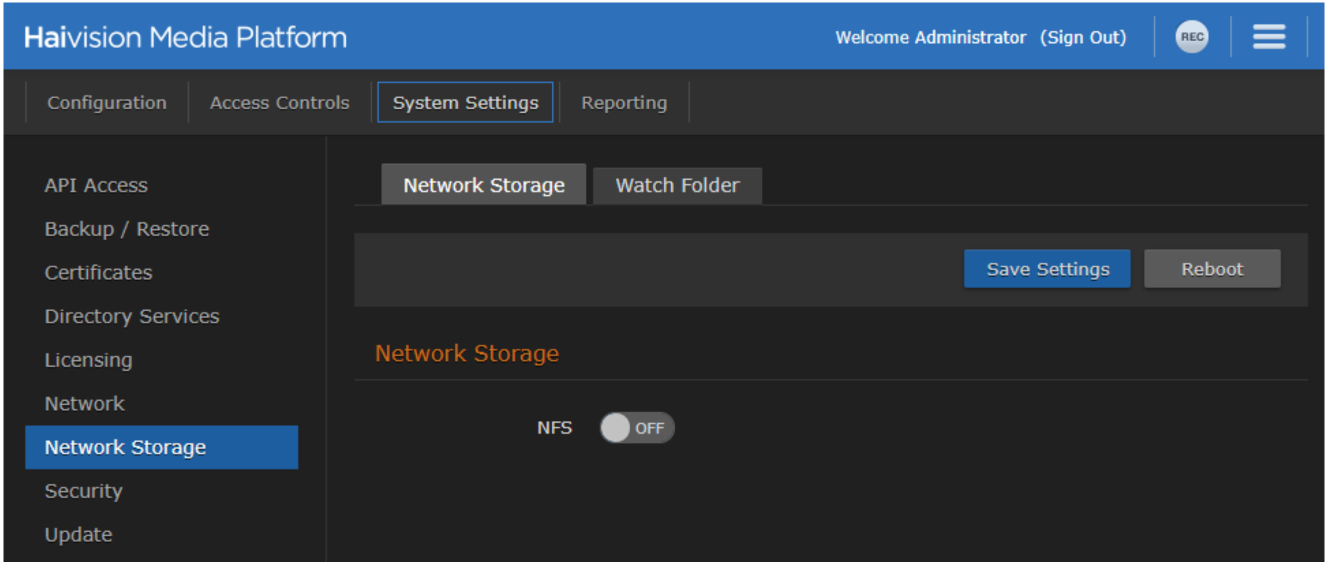
**When setting up Haivision Media Platform, you may (optionally) configure a range of network storage settings.**

## Configuring Network Storage

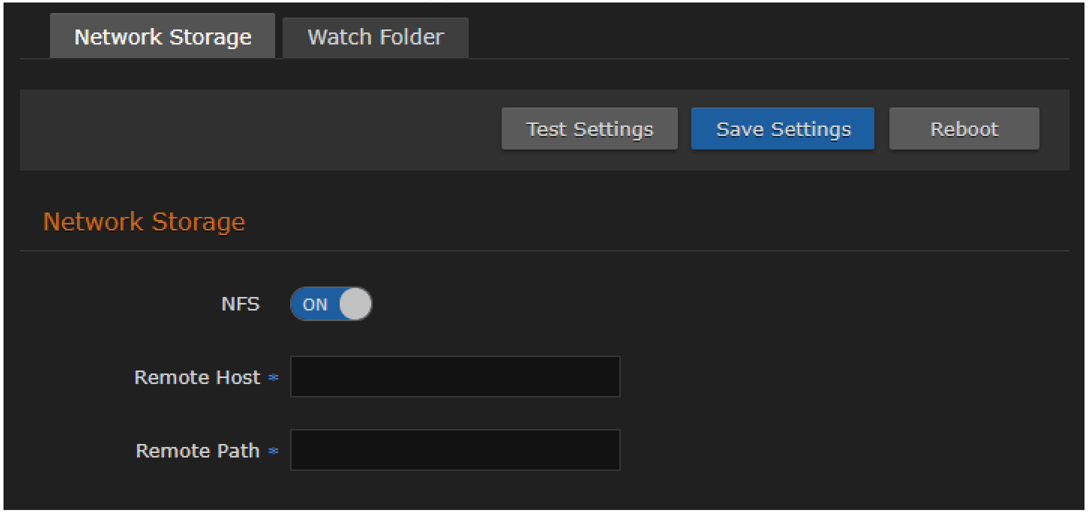
Network Storage is a licensed option that enables you to move video storage from your HMP server to Network-Attached Storage (NAS) through a Network File System (NFS) connection.

To configure network storage:

1. On the Administration screen, click **System Settings** on the toolbar and then click **Network Storage** on the sidebar.
   The Network Storage pane opens.



2. To connect to an NFS server, toggle the **NFS** button to **On**.



Network Storage Watch Folder

Test Settings Save Settings Reboot

Network Storage

NFS ON

Remote Host *

Remote Path *

3. Fill in the remote host IP address and path
4. To test the connection from HMP to the defined NFS server, click **Test Settings**.
5. Click **Save Settings** to save the connection.
6. Click **Reboot** to restart the HMP server
7. After the reboot, click **Migrate** to copy your videos to the NFS server.
   The progress bar shows the progress of the migration.
   Your videos will now be 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).

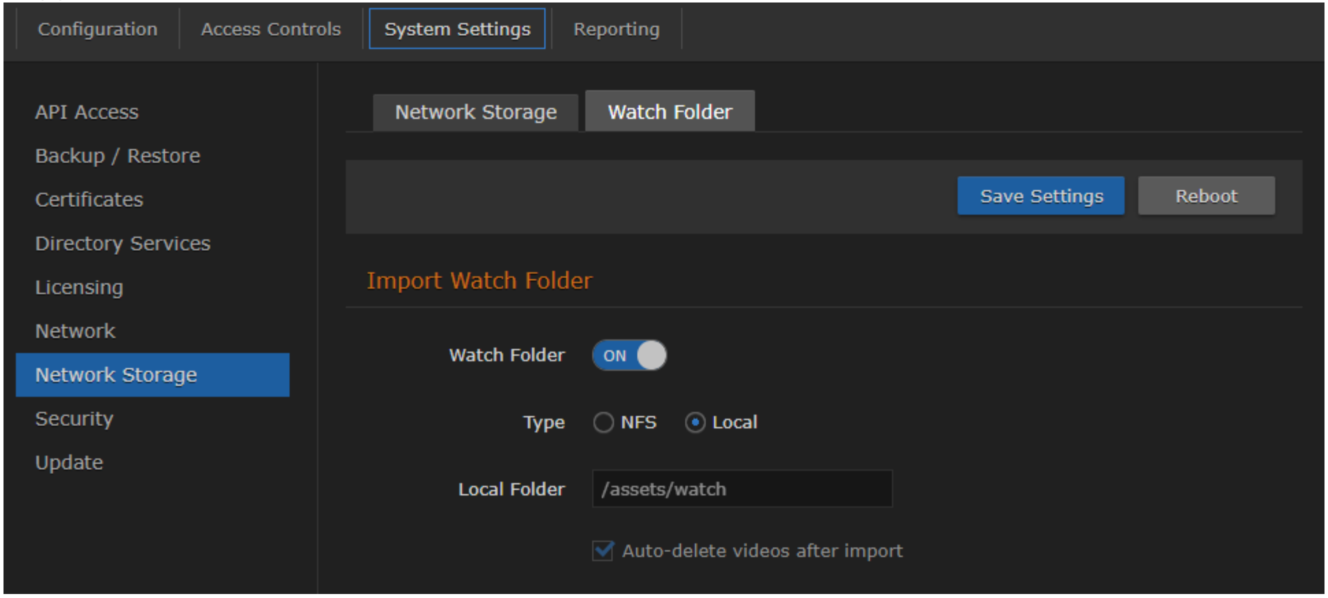
HMP watch folders also support import/ingest of XML sidecar metadata for media assets, and XMLTV files with custom EPG data.

**Note**

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

**To configure a watch folder:**

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



Watch Folder: ON
Type: ○ NFS ● Local
Local Folder: /assets/watch
☑ Auto-delete videos after import

3. Select the folder type (either NFS or Local). 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 Remote Path.
4. Click **Save Settings** to save the connection.
5. Click **Reboot** to restart the HMP server.

**Tip**

To automatically import from a Makito X with Storage: The Makito X export manager will create a folder named "recordings" on the Makito X-configured external storage (NFS or FTP). From HMP, you need to 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 (formerly named "Calypso") XML files while editing existing assets or assets that are in the process of being imported. Metadata imported from the HMP XML file will completely overwrite 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 will be 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 | Contains the description with HTML tags and embedded images. |
| ctime | optional | The source creation time: Unix timestamp (seconds). |
| mtime | ignored | The source's last modified time: Unix timestamp (seconds).<br>Importing an HMP XML file causes the asset's `mtime` to be updated 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.<br>If included, all metadata including HotMarks will be 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 do 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 will be 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 will no longer show up as a related asset on any session.
- `calypso:creator` – If the creator does not exist, it will not show up under the "Mine" Browse Content filter for anyone.
- `calypso:expiration_timestamp`
- `calypso:recordGeoaddress`
- `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 will be returned and the XML import will fail. However, if the asset does not have a duration, the XML import will succeed. This can happen when the asset itself is still being imported and no duration can be calculated yet. If the imported asset turns out to have a duration less than the HotMark, then that HotMark timestamp will not be visible on the player, but will show up on the `/assets/:id/hotmarks` API.

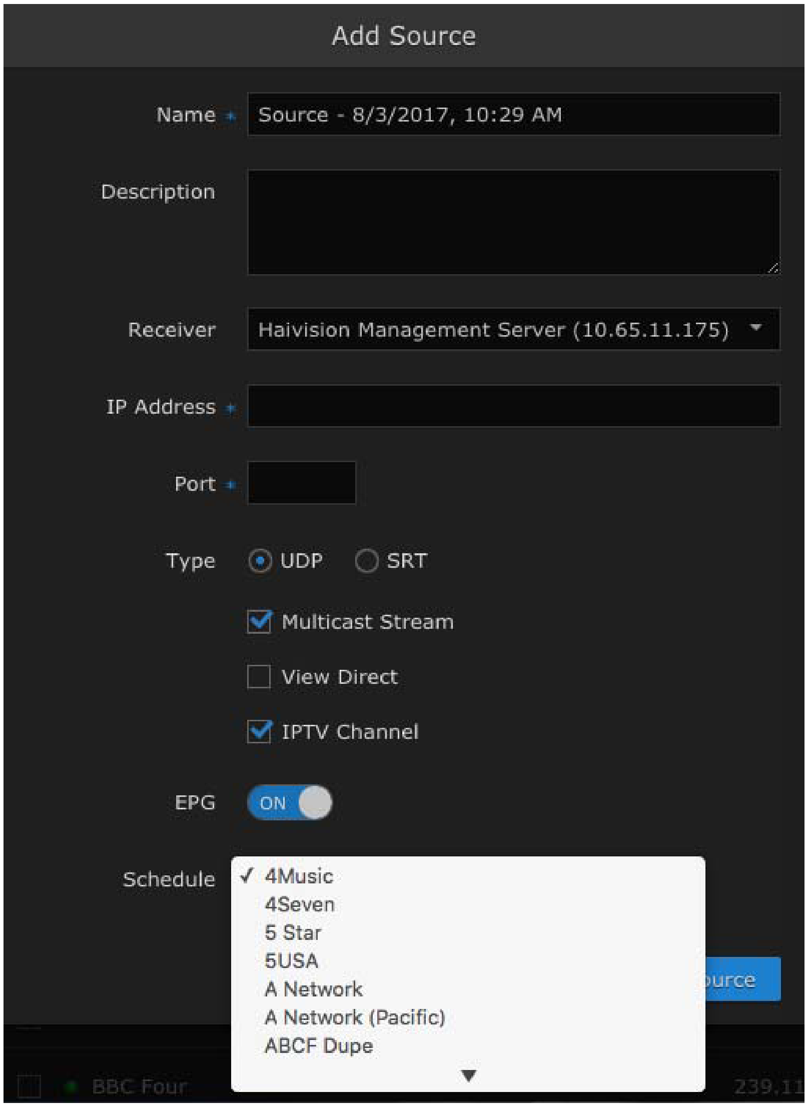
## Example Calypso XML File

```
<?xml version="1.0" encoding="UTF-8"?>
<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:recordGeoaddress</name>
        <field>
          <type>STRING</type>
          <value>4445 Rue Garand:Montréal:QC:H4R2H9:Saint-Laurent:Rue Garand:4445:Canada</value>
        </field>
      </entry>
      <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&gt;Test&lt;/b&gt;&lt;div&gt;&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 the XMLTV format.

When the watch folder feature is enabled, HMP automatically creates an `/xmltv` directory within `/watch`. When you upload a plain .xml file containing the XMLTV data, or a .tar.gz archive containing multiple such .xml files to the `/watch/xmltv` folder, HMP will detect the upload, wait for 20 seconds for it to complete, and then ingest the file(s). Once processed, the custom EPG channels will be available to be scheduled in a Source (added to the existing channel list, if any):



Add Source

Name * Source - 8/3/2017, 10:29 AM

Description

Receiver Haivision Management Server (10.65.11.175)

IP Address *

Port *

Type ● UDP ○ SRT

☑ Multicast Stream

□ View Direct

☑ IPTV Channel

EPG ON

Schedule

**Note**

Both read and write permissions must be set on any files uploaded to the `/xmltv` folder, or the import will fail. Once 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="20170729000000 +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 here: http://wiki.xmltv.org/index.php/XMLTVFormat

## Managing Security

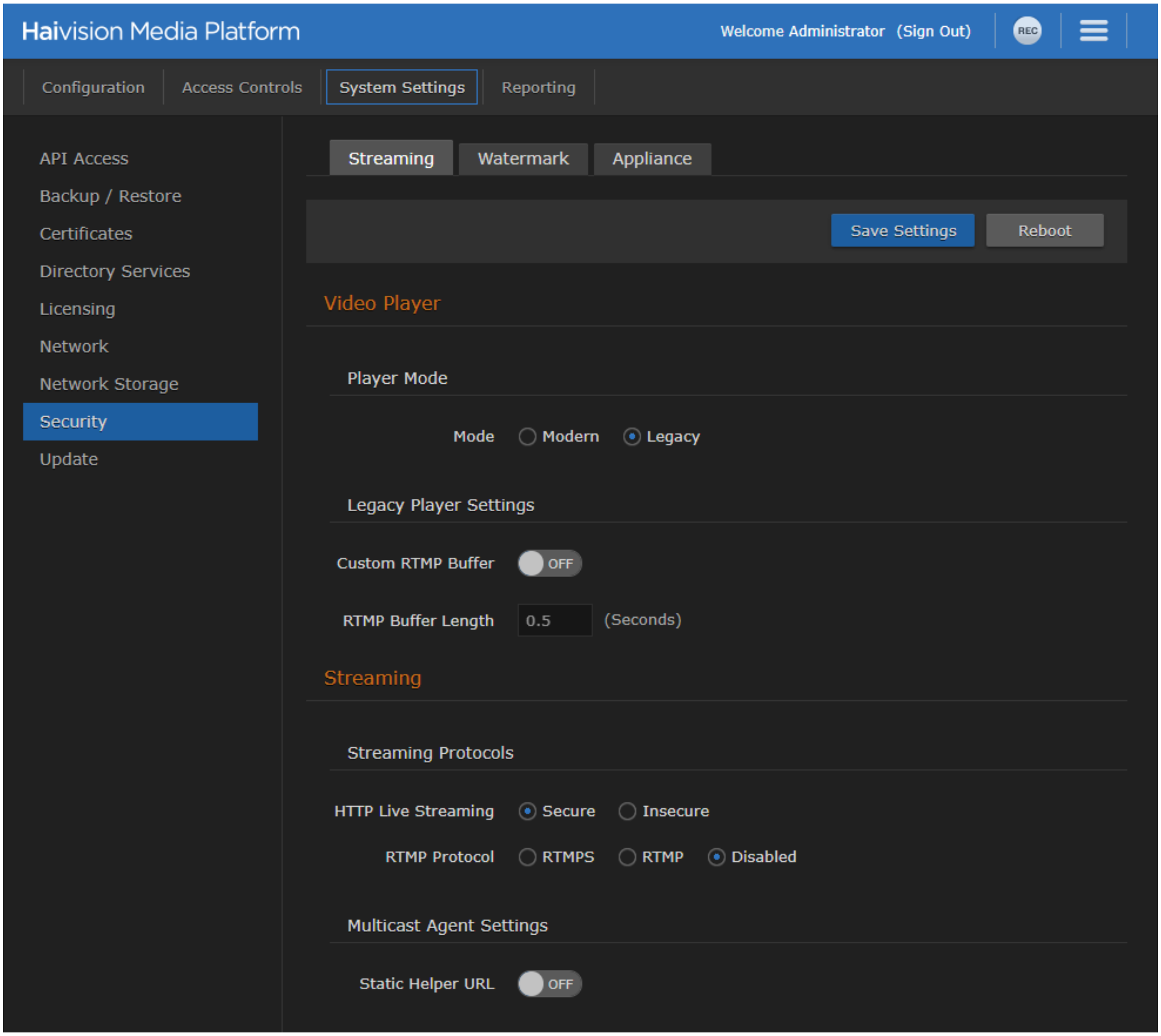
When setting up Haivision Media Platform, you may (optionally) configure a range of security settings.

### Configuring Secure Streaming

HMP supports encrypted streaming from the appliance to the desktop. From the Streaming pane, you can also set desktop browser playback to either "Modern" or "Legacy". The "Modern" player is a native HTML5 player (via HLS), while the "Legacy" player is a Flash-based player.

To enable encrypted streaming:

1. On the Administration screen, click **System Settings** on the toolbar and then click **Security** on the sidebar.



Video Player

Player Mode

Mode ○ Modern ● Legacy

Legacy Player Settings

Custom RTMP Buffer OFF

RTMP Buffer Length 0.5 (Seconds)

Streaming

Streaming Protocols

HTTP Live Streaming ● Secure ○ Insecure

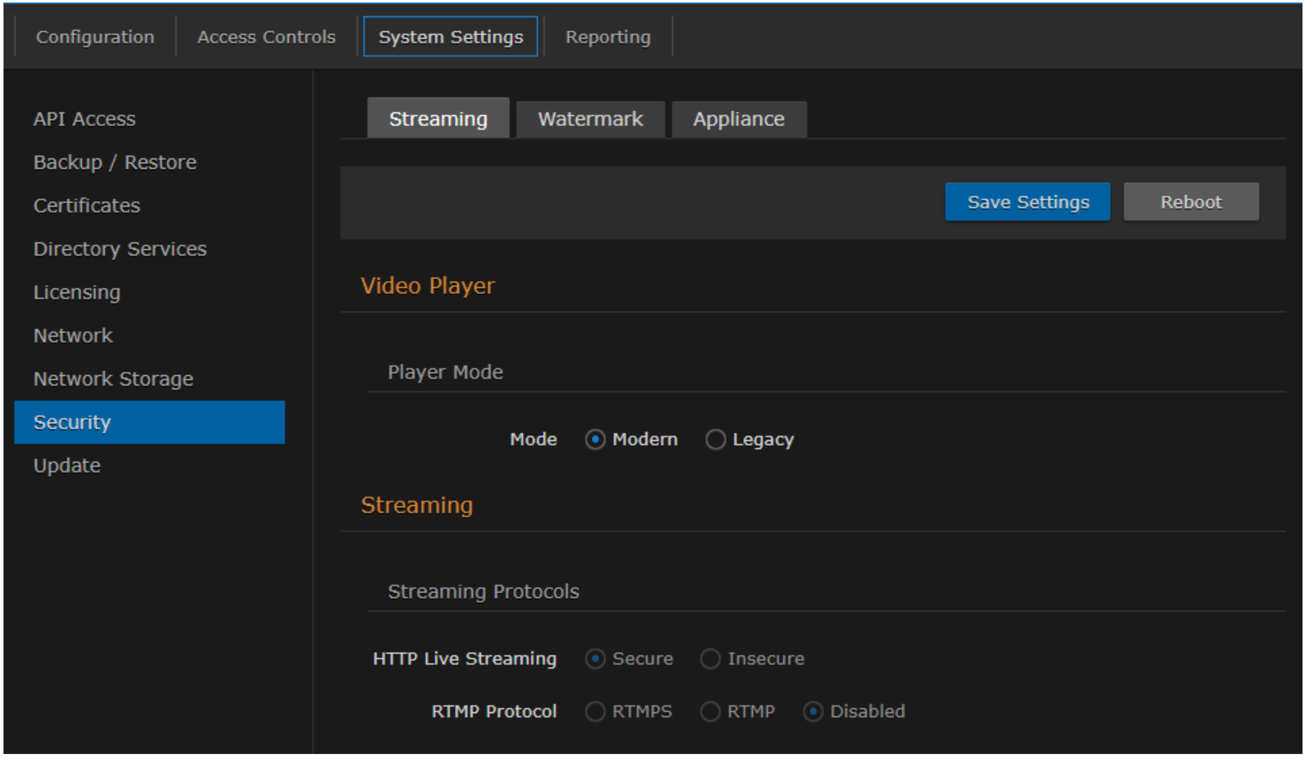
RTMP Protocol ○ RTMPS ○ RTMP ● Disabled

Multicast Agent Settings

Static Helper URL OFF

2. Select the Streaming Protocol, either RTMPS, RTMP, RTMFP or HLS. See the Streaming Protocols entry in Security Settings.
3. (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.

4. To switch the Player Mode between the HTML5 and Flash-based players, select either “Modern” or “Legacy”. See Player Mode under **Security Settings**.



Video Player

Player Mode

Mode ● Modern ○ Legacy

Streaming

Streaming Protocols

HTTP Live Streaming ● Secure ○ Insecure

RTMP Protocol ○ RTMPS ○ RTMP ● Disabled

5. Click **Save Settings**.
6. Click **Reboot** to restart the HMP server.

**Topics Discussed**

- Configuring a Watermark
- Configuring Appliance Security
- Security Settings

## Configuring a Watermark

**Important**

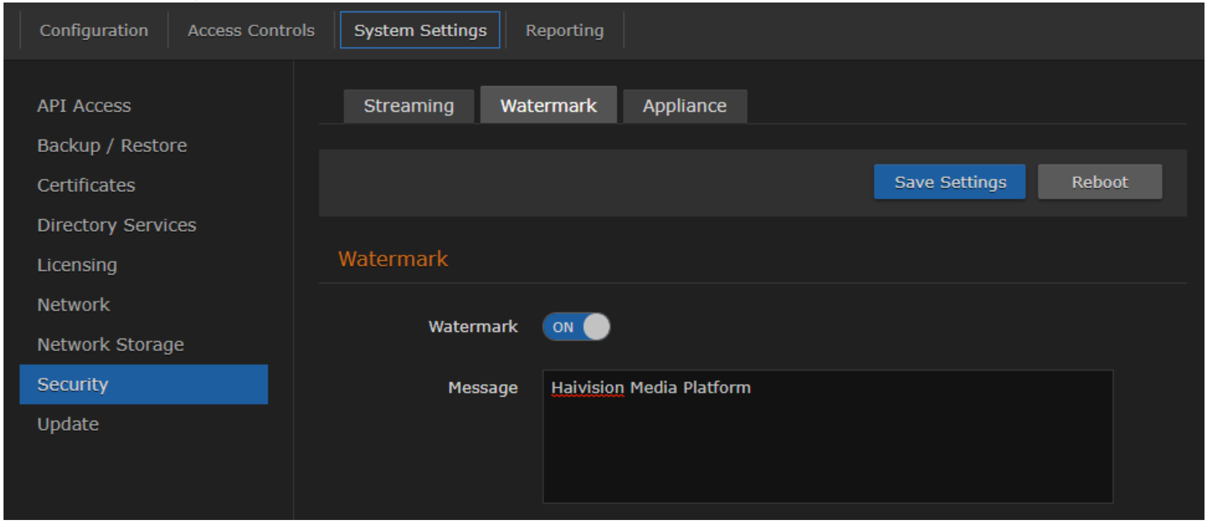
The watermark feature is not compatible with the modern player. Enabling both can cause erratic behavior (e.g., the video might play without a watermark or fail to play altogether).

**Note**

By default, HLS access is disabled and RTMP is used for VOD when watermarking is enabled. See the Watermark entry in **Security Settings**.

**To configure a watermark:**

1. On the Security pane, click the **Watermark** tab.



Watermark

Watermark ON

Message Haivision Media Platform

2. Toggle the Watermark button to **On**. See the Watermark entry in **Security Settings**.
3. Type or copy in the text to display in the watermark.
4. Click **Save Settings**.
5. Click **Reboot** to restart the HMP server.

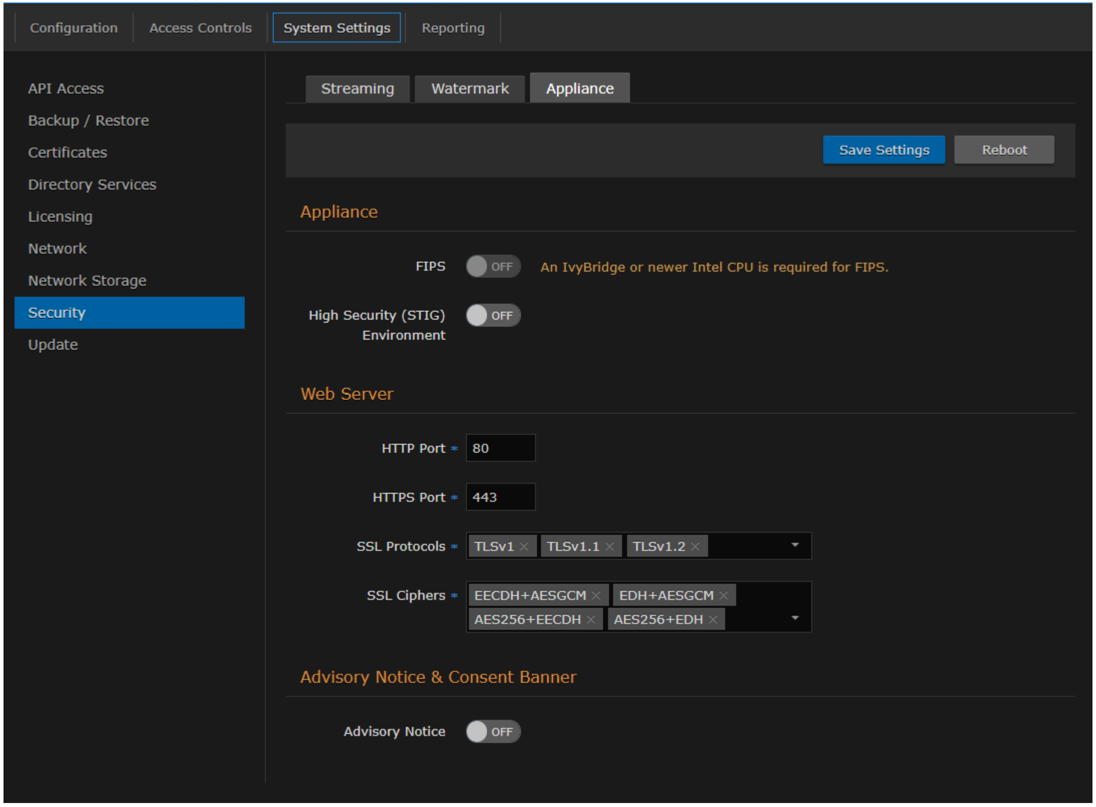
## Configuring Appliance Security

From the Appliance pane, you may (optionally) configure additional system security hardening settings and a security banner:

- > **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 pane, click the **Appliance** tab.



Appliance

FIPS OFF An IvyBridge or newer Intel CPU is required for FIPS.

High Security (STIG) Environment OFF

Web Server

HTTP Port * 80

HTTPS Port * 443

SSL Protocols * TLSv1 × TLSv1.1 × TLSv1.2 ×

SSL Ciphers * EECDH+AESGCM × EDH+AESGCM × AES256+EECDH × AES256+EDH ×

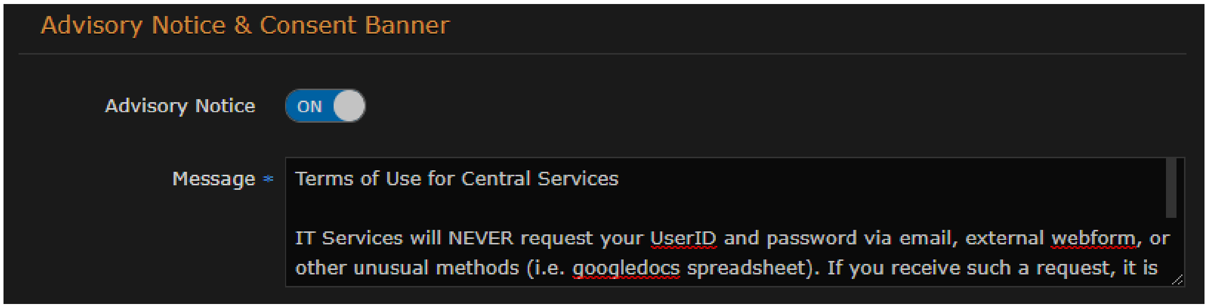
Advisory Notice & Consent Banner

Advisory Notice OFF

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

> **Important**
>
> Changes to port numbers take effect immediately. Changing port numbers will affect ongoing operations using the service at that port.

5. To configure a banner, type or copy in the desired banner text. Toggle the **Advisory Notice** button to **On**.



Advisory Notice & Consent Banner

Advisory Notice ON

Message * Terms of Use for Central Services

IT Services will NEVER request your UserID and password via email, external webform, or other unusual methods (i.e. googledocs spreadsheet). If you receive such a request, it is

6. Click **Save Settings** to save the connection.
7. Click **Reboot** to restart the HMP server.

> **Note**
>
> All settings except for Web Server require a reboot.

## 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.

Streaming Watermark Appliance

### Streaming

| Setting | Description |
|---|---|
| **Video Player** | |
| Player Mode | To switch desktop browser playback between the HTML5 and Flash-based player, select either:<br>• Modern: The Modern player is 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.<br>The Modern player may require slightly more buffering time than the Legacy player, due to differences in HLS vs. RTMP. Also, KLV and Watermarking are not supported with the modern player.<br>Protocol must be set to HLS and HTTP Live Streaming (HLS) must be Secure.<br>• Legacy: This is the existing flash-based player. Newly installed systems as well as systems upgraded to v2.6 or greater will default to the Legacy player.<br>Player Mode is a system-wide setting. |
| Legacy Player Settings | (Player Mode must be Legacy) |
| Custom RTMP Buffer | To tune the Flash video buffer to smooth out playback, toggle the Custom RTMP Buffer button to **On**. |
| RTMP Buffer Length | Type in the buffer length. Range: 0.5..5 seconds. |
| **Streaming Protocols** | |
| HTTP Live Streaming (HLS) | Choose whether HMP will use secure (encrypted) or insecure (unencrypted) mode for HLS streaming. Set to "Secure" by default.<br>• Secure: Select to ensure that users cannot stream on a mobile device without a valid security certificate.<br>• Insecure: Select to allow users to stream on a mobile device without a valid security certificate.<br>**Note**<br>If you select Secure, some mobile devices (notably iPhone/iPad) cannot display the stream unless you have a valid SSL certificate in place. |

| | |
|---|---|
| RTMP Protocol | Choose whether HMP will use a plain or secure streaming protocol:<br>• RTMPS: Select to enable secured RTMP. Real-Time Messaging Protocol (RTMP) Secure encryption uses SSL (Secure Sockets Layer) certificates to encrypt the traffic for the Web browser. HMP ships with a self-signed SSL certificate which will work 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.<br>When accessing the Web interface, users will 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.<br>**Important**<br>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.<br>• RTMP: Select to enable standard RTMP.<br>• Disabled: Select to disable RTMP. |
| **Multicast Agent Settings** | |
| Static Helper URL | To specify a fixed hostname for the multicast agent download, toggle the Static Helper URL button to **On**.<br>**Note**<br>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.)<br>For more information, refer to “Haivision Media Platform Integration” in the **Haivision Helper Installation Guide**. |

Streaming Watermark Appliance

### Watermark

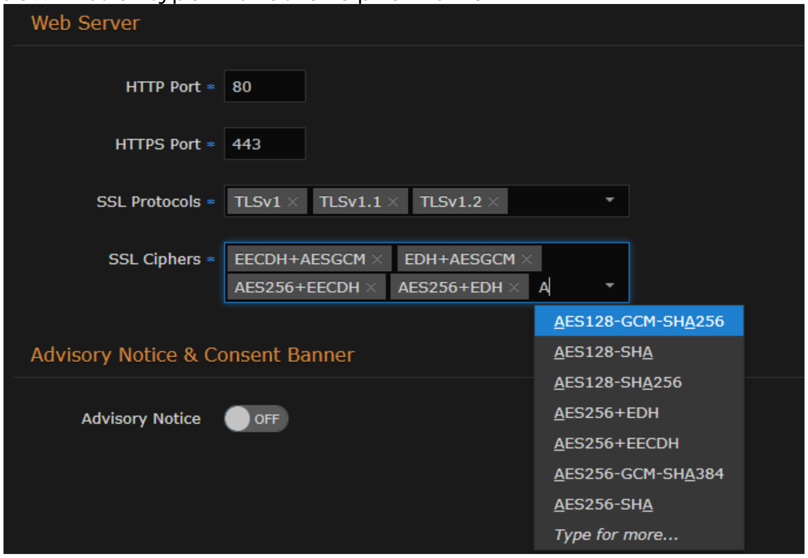
| Setting | Description |
|---|---|
| Watermark | (Player Mode must be Legacy) To configure a system-wide, static message to be displayed as an overlay on all videos played back in the user's authenticated HMP Web browser, toggle the **Watermark** button to **On**. Then copy or type in the text to display.<br>**Important**<br>The watermark is a player feature and is not embedded in the video. In order to ensure secure delivery of the video to the player, use RTMP or RTMPS for the Browser delivery (see “RTMP Protocol” under **Streaming**). |

Streaming Watermark Appliance

### Appliance

| Setting | Description |
|---|---|

| | |
|---|---|
| **Appliance** | |
| FIPS | 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.<br>**Note**<br>To use FIPS mode, the CPU must be an IvyBridge or newer Intel CPU with the RDRAND instruction. |
| Lock Session After | (High Security (STIG) Environment must be Legacy) Type in the time period (in minutes) allowed for inactivity before an HMP session is locked (on all interfaces, console, ssh, and Web). |
| High Security (STIG) Environment | To enable security hardening features for high-security environments, toggle this button to On. This setting includes:<br>• Session timeouts/locks for all interfaces.<br>• Stronger password requirements<br>• Lock/disable accounts due to multiple authentication failures or expired passwords.<br>• Disabling unnecessary services.<br>**Note**<br>This complies with National Institute of Standards and Technology (NIST) Special Publication 800-53 (see https://nvd.nist.gov/800-53/ Rev 4).<br>**Important**<br>Only security professionals who understand the cipher support and requirements within their organization should change this setting.<br>Some of these settings are not supported by Haivision Play Set-Top Box or by Google Chrome.<br>The default list has been verified for broad acceptance, and should typically only be adjusted to mitigate new and critical vulnerabilities that may occur. |
| Lock Session After | (High Security (STIG) Environment must be Legacy) Type in the time period (in minutes) allowed for inactivity before an HMP session is locked (on all interfaces, console, ssh, and Web). |
| **Web Server** | |
| HTTP Port<br>HTTPS Port | To configure the Web port for HMP:<br>• HTTP Port number (Default = 80)<br>• HTTPS Port number (Default = 443)<br>**Important**<br>If you change the HTTP/HTTPS ports, any connected STBs will lose connection and need to be redirected to the new HTTP 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. |
| SSL Protocols | To specify which TLS (Transport Layer Security) versions are accepted, select from the drop-down list: TLS v1, TLS v1.2, TLS v1.2. |

| | |
|---|---|
| SSL Ciphers | To specify which SSL Ciphers are accepted, select from the drop-down list or type in another cipher name:<br><br>Web Server<br>HTTP Port * 80<br>HTTPS Port * 443<br>SSL Protocols * TLSv1 × TLSv1.1 × TLSv1.2 ×<br>SSL Ciphers * EECDH+AESGCM × EDH+AESGCM × AES256+EECDH × AES256+EDH × A<br>AES128-GCM-SHA256<br>AES128-SHA<br>AES128-SHA256<br>AES256+EDH<br>AES256+EECDH<br>AES256-GCM-SHA384<br>AES256-SHA<br>*Type for more...*<br>Advisory Notice & Consent Banner<br>Advisory Notice OFF |
| **Advisory Notice & Consent Banner** | |
| Advisory Notice | When enabled, the banner will appear when users sign in (console, SSH and Web interface) and remain on the screen until the administrator 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.<br>To enable the banner (as shown in the text box), toggle the **Advisory Notice** button to **On**.<br>Type or copy the banner text into the text box. |

## Installing System Updates

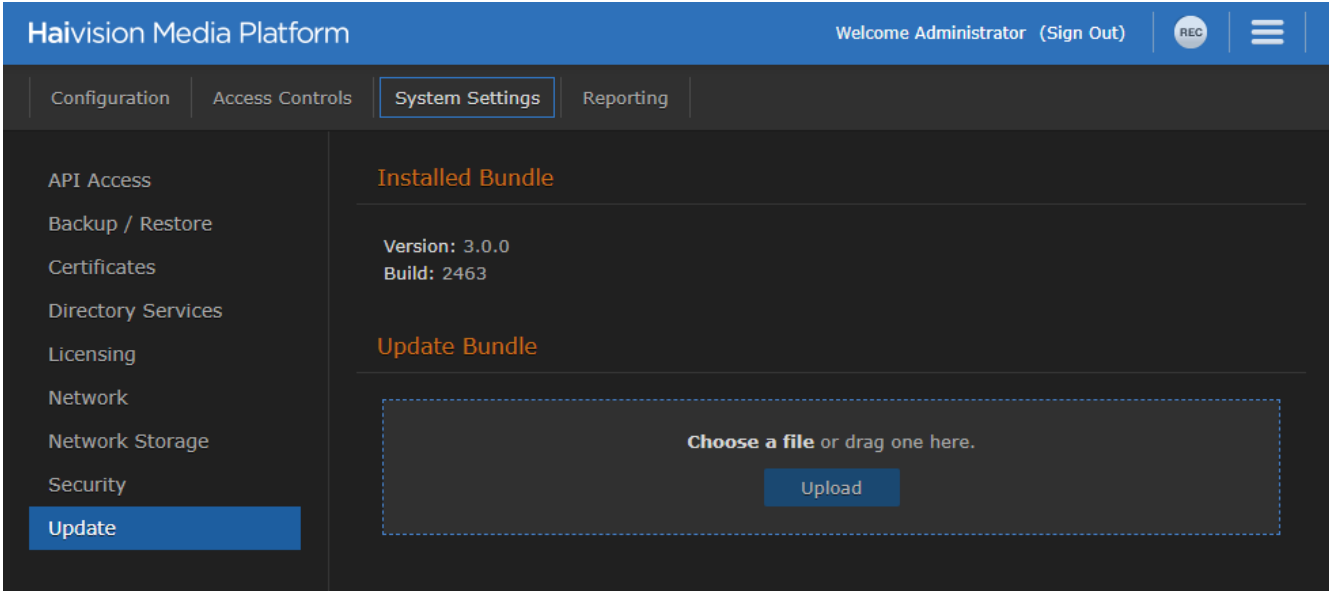
When you first receive the Haivision Media Platform appliance, the necessary software is pre-installed on it. System updates are issued through Haivision's Support Portal on our website at: https://support.haivision.com.

> **Note**
>
> For major releases or when adding new features, you need to apply a valid license key before or after the update (see Managing Licenses). 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.

**The system update is entitled `calypso-xxxxx_rxxxxx_release.hai`, which when loaded replaces the application on your HMP.**

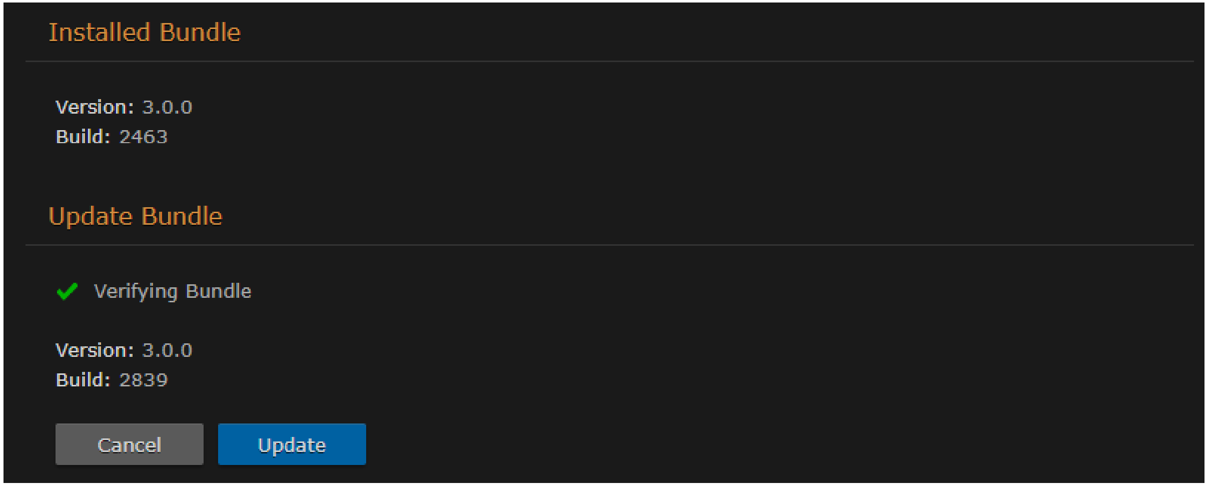
To install a system update:

1. On the Administration screen, click **System Settings** on the toolbar and then click **Update** on the sidebar. The Update pane opens:



Version: 3.0.0
Build: 2463

2. Drag an update bundle to the drop area or click **Choose a file** to select a bundle to load.
3. After you select the bundle, a confirmation appears showing the filename. Click **Upload** to continue. The progress bar shows the progress of the upload.
4. After the bundle is uploaded and verified, click **Update** and then click **Confirm**.



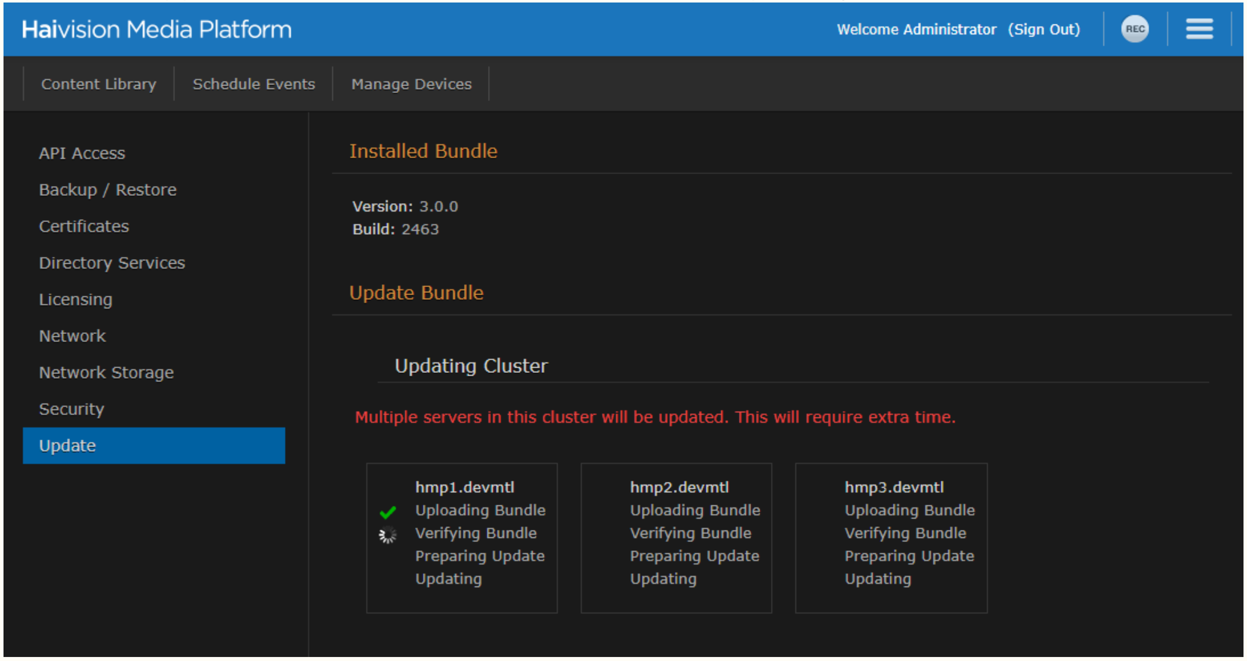
Version: 3.0.0
Build: 2463

✓ Verifying Bundle

Version: 3.0.0
Build: 2839

**Note**

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



Installed Bundle

Version: 3.0.0
Build: 2463

Update Bundle

Updating Cluster

Multiple servers in this cluster will be updated. This will require extra time.

| hmp1.devmtl | hmp2.devmtl | hmp3.devmtl |
|---|---|---|
| ✓ Uploading Bundle<br>Verifying Bundle<br>Preparing Update<br>Updating | Uploading Bundle<br>Verifying Bundle<br>Preparing Update<br>Updating | Uploading Bundle<br>Verifying Bundle<br>Preparing Update<br>Updating |

5. Wait until the update is complete and the appliance restarts.
6. After the appliance restarts, the browser displays the HMP Sign-in screen (depending on your Web browser and settings). If not, reload your browser.
7. Sign in and ensure the system is functional.
8. 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:
   a. On the Administration screen, click **System Settings** on the toolbar and click **Network Storage** on the sidebar.
   b. Under Network Storage Migration, click the **Migrate** button.
   c. 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.

# Reporting

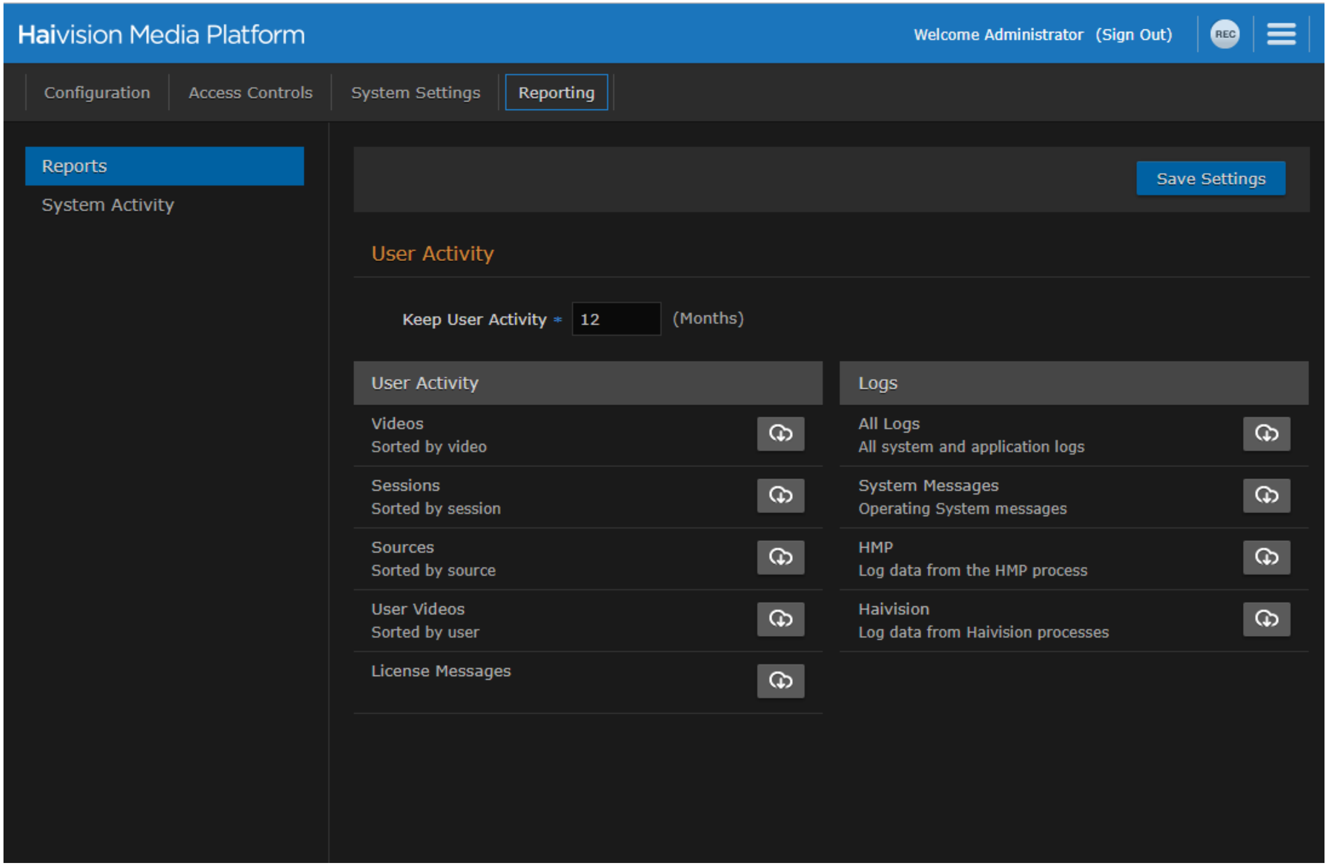
The Administration Reporting screen includes two panes: Reports and System Activity.

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.

## Viewing Reports

To view the reports:

1. To navigate the Administration screen, click the ☰ icon on the banner and select **Administration** from the navigation drop-down menu.
2. On the Administration screen, click **Reporting** on the toolbar and then click **Reports** on the sidebar.



Keep User Activity * 12 (Months)

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

> **Note**
>
> User activity data older than the specified time period will be 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 table lists the available reports and logs:

| Report/Log Item | Description |
|---|---|
| User Activity | A list of user activities (in.CSV file format). For each activity, the list shows the following:<br>• ID of the user performing the activity (for Web viewers) or the device ID (for STBs),<br>• uuid of the associated item,<br>• start time of the activity,<br>• name or title of the item,<br>• the action taken (WATCH, DOWNLOAD, EDIT, SHARE, DELETE, etc.),<br>• a URL link to launch it, and<br>• stime or start time in extended ISO format<br>**Note**<br>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. |
| Videos | **Note**<br>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 | **Note**<br>The Sources report logs all source viewing activity. It is intended to log user activity and STB activity. |
| User Videos | Activities sorted by user. |

| | |
|---|---|
| License Messages | **Note**<br>After the initial occurrence, a new occurrence is reported only after the bandwidth has dropped and then when licensed bandwidth has been exceeded again.<br>The report includes data Type, Time, and Message, for example, “ `Output bandwidth limit reached (bps): total usage:8629400( babel:8629400 hls:0 ), max allowed:8000000.` ” |
| **Logs** | |
| 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. |

# Viewing System Activity

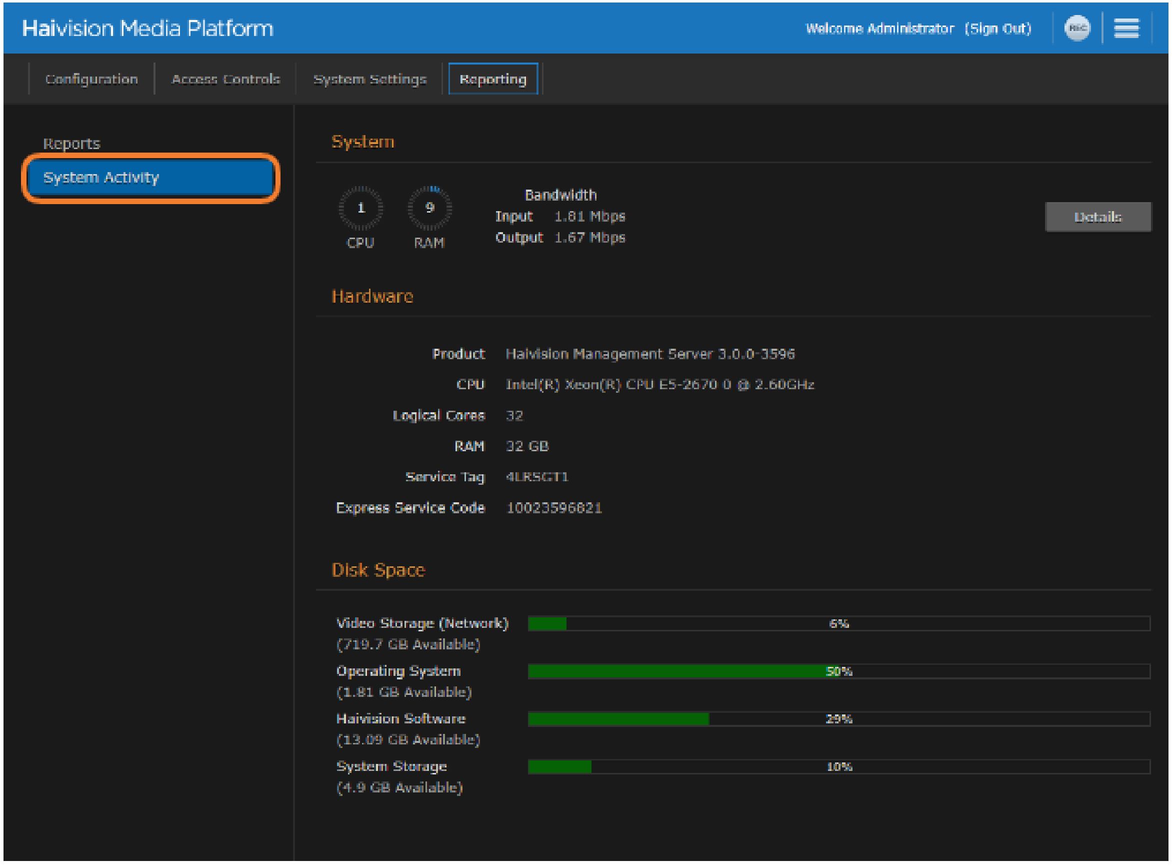
The System Activity pane summarizes real-time System Status information, such as CPU and Memory usage, and Input and Output bandwidth bitrates, with the option to open a Details panel.

The Hardware summary provides hardware details including whether HMP is running on a VM or a Haivision "appliance".

> **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. On the Administration screen, (if necessary) click **Reporting** on the toolbar and then click **System Activity** on the sidebar.



Bandwidth
Input 1.81 Mbps
Output 1.67 Mbps

| | |
|---|---|
| Product | Haivision Management Server 3.0.0-3596 |
| CPU | Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz |
| Logical Cores | 32 |
| RAM | 32 GB |
| Service Tag | 4LRSGT1 |
| Express Service Code | 10023596821 |

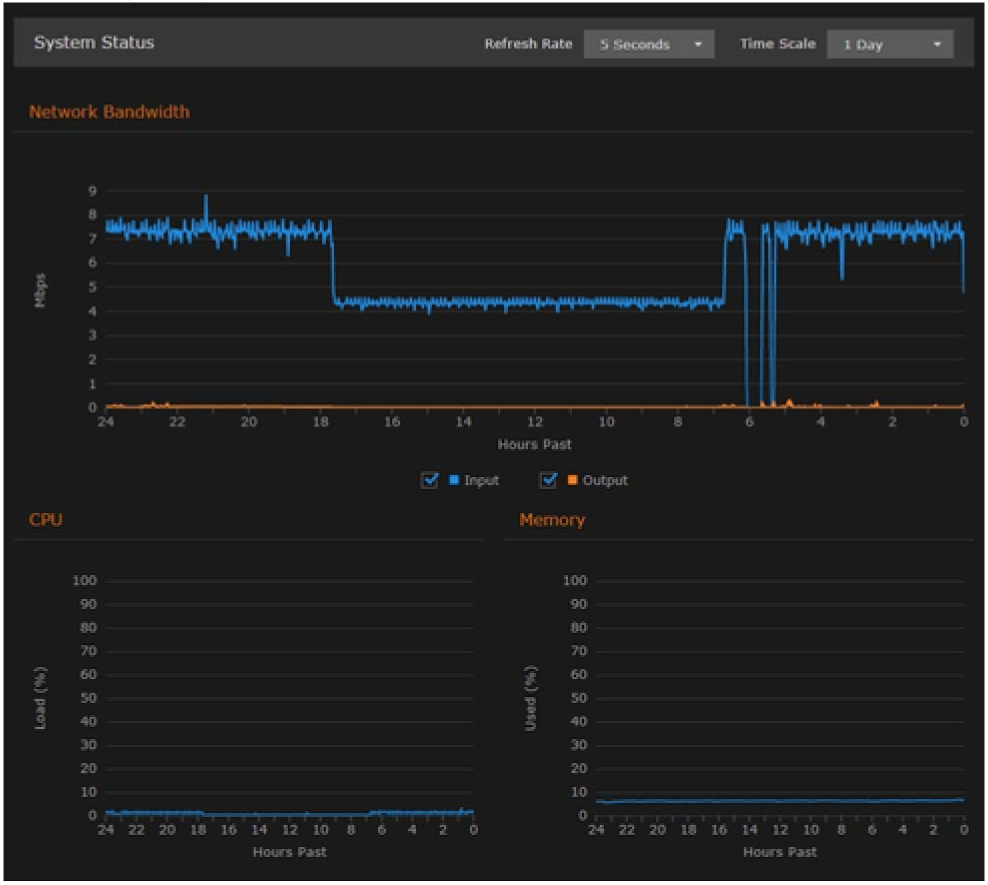
| | |
|---|---|
| Video Storage (Network)<br>(719.7 GB Available) | 6% |
| Operating System<br>(1.81 GB Available) | 50% |
| Haivision Software<br>(13.09 GB Available) | 29% |
| System Storage<br>(4.9 GB Available) | 10% |

> **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%.

2. To view the Network Bandwidth, CPU, and Memory graphs, 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 (megabits per second)
- CPU (Load) Usage (percentage)
- Memory Usage (percentage used)

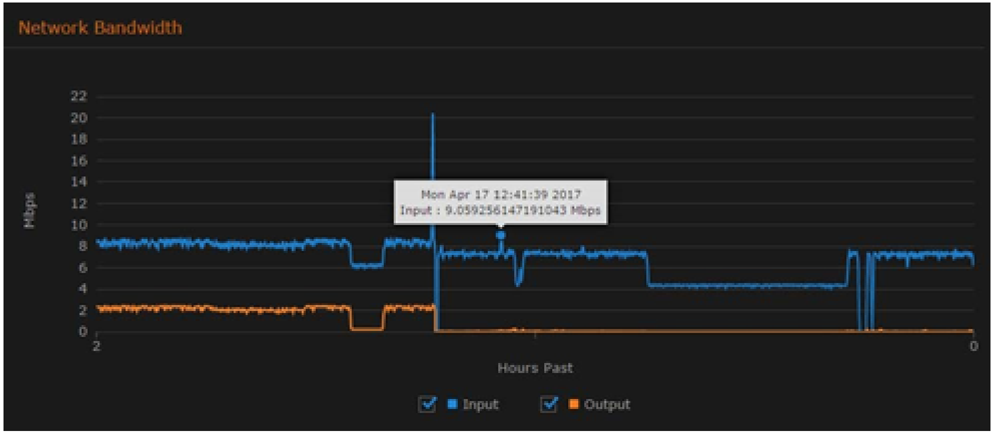


System Status

Refresh Rate: 5 Seconds

Time Scale: 1 Day

3. 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.
4. To fine-tune the Bandwidth usage graph, select the data to include: Input and/or Output (playback).
5. To display an exact reading for the time and usage, you can mouse over the any of the graph lines, as shown in the following example.



Mon Apr 17 12:41:39 2017
Input : 9.059256147191043 Mbps

**Related Topics**

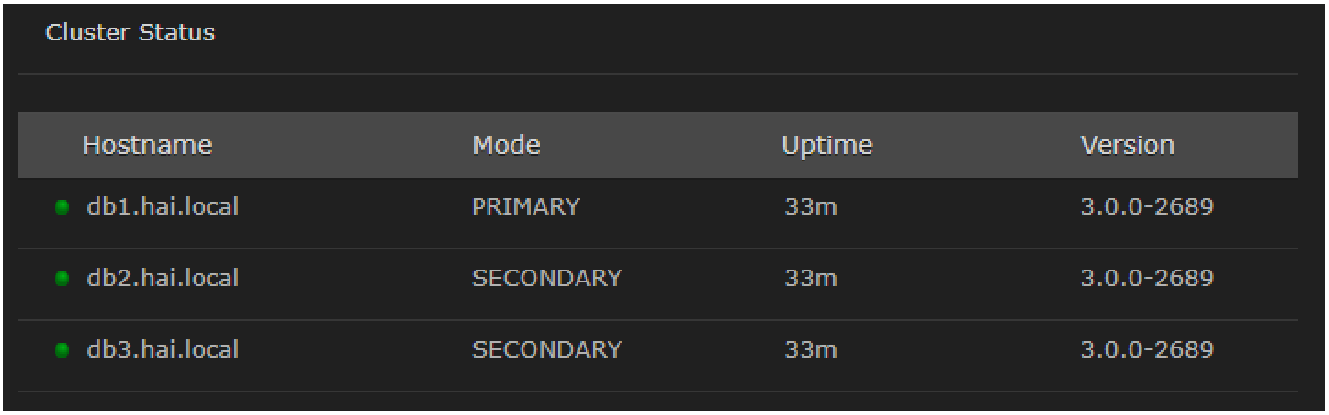
- Viewing High Availability Cluster Status

## Viewing High Availability Cluster Status

If your system has High Availability (HA) clustering support and you are logged in as an administrator, 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

**Note**

A sample dictionary file is available from the Haivision Support Portal at: https://support.haivision.com

**Topics Discussed**

## 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.

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:

```
{
  "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.

format:

```
{
  "type": "item",
  "key": "13",
  "format": "int32",
  "translation": {
    "multiplier": 4.1909515877212172316951757444512e-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.

### Item - Enum - Values

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"
}
```

### Item - Enum - Bits

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 didn't 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 doesn't support 64-bit integers.

# Technical Specifications

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

**Topics Discussed**

## Haivision Media Platform (All Systems)

| | |
|---|---|
| **Management Interfaces** | HMP Portal<br>REST API<br>Command Line API<br>Console UI |
| **Features** | Session-based workflow<br>Access control<br>HotMarks insertion with annotation<br>API-enabled control<br>Multi-source recording<br>Real-time streaming & sharing<br>No software installation |
| **Inputs** | MPEG Transport Stream<br>H.264<br>ADTS AAC Audio |
| **Output** | RTMP, RTMPS, RTMFP, MPEG Transport Stream |
| **Platform** | Secure Linux-based OS |

## Haivision Media Platform - 1RU

| **Physical Specifications** | |
|---|---|
| **Hardware Platform** | Haivision optimized server platform (1RU)<br>1.8 TB RAID 5 |
| **Physical Characteristics** | Intel-based processing |
| **Power Supplies** | 2 x 550 W hot swappable |
| **Dimensions (H x W x D)** | 42.5H x 431W x 642D (mm) |
| **Weight** | >(Maximum config) 19.9 kg (43.87 lbs.) |
| **Environmental Specifications** | |

| | |
|---|---|
| **Temperature (Operating)** | 10° to 35°C (50° to 95°F) |
| **Relative Humidity (Operating)** | 10% to 80% (noncondensing) |

## Haivision Media Platform - 2RU

| **Physical Specifications** | |
|---|---|
| **Hardware Platform** | Haivision optimized server platform (2RU)<br>6.6 TB RAID 5 |
| **Physical Characteristics** | Intel-based processing |
| **Power Supplies** | 2 x 750 W hot swappable |
| **Dimensions (H x W x D)** | 86.4H x 431W x 722.8D (mm) |
| **Weight** | (Maximum config) 32.5 kg (71.5 lbs.) |
| **Environmental Specifications** | |
| **Temperature (Operating)** | 10° to 35°C (50° to 95°F) |
| **Relative Humidity (Operating)** | 10% to 80% (noncondensing) |

# 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, Havision 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 | • Access to all functions through the administrative user interface.<br>• Ability to add or modify objects and metadata through the application programming interface (“API”)<br>• Ability of ingest service to check for new or updated files or feeds | 99.999% |
| Read-Only Functions | • Ability to retrieve data through the API<br>• Ability for Audience Members to authenticate through the Access Service<br>• Ability for Audience Members to play Published Media Objects<br>• Ability for Audience Members to play Haivision VCMS-authenticated or entitled Published Media Objects<br>• 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 | • Preventive maintenance on the software/ hardware components of Haivision VCMS<br>• Addition of new features/functions<br>• Repair errors that are not immediately affecting Your use of Haivision VCMS | No | Yes | 10 Hours | 6 Hours | 10:00pm - 5:00am | 48 Hours |
| Urgent | • 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 | • 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<br>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

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

info@haivision.com
www.haivision.com

North America: 1.877.224.5445
International: +1.514.334.5445

HAIVISION