Haivision

Media Gateway 1.4.1
User's Guide

HVS-ID-UG-MGW-1.4.1, Issue 01

Table of Contents

Edition Notices

This edition notice provides important information regarding the documentation for Media Gateway version 1.4.1. Later releases are intended to be backwards-compatible, but may introduce new functionality not addressed in this content. Likewise, other product documentation may describe functionality not addressed here that will become available in later releases. Please consult with Haivision Systems, Inc. or its authorized representatives to ensure compatibility.

Copyright

Title: Media Gateway User's Guide
Document Number: HVS-ID-UG-MGW-1.4.1
Issue Number: 01

Trademarks

Disclaimer

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

If you have comments or suggestions, please contact:

Haivision
ATTN: Information Development
4445 Garand
Montréal, Québec, H4R 2H9 Canada

Telephone: 1-514-334-5445

Email: info@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. The latest information available can be acquired from our web portal at: http://www.haivision.com/download-center/

NOTE

A login is required to access the Haivision Download-Center.

About This Content

Welcome to the Media Gateway Version 1.4.1 User's Guide. This document describes how to configure and manage the Haivision Media Gateway.

Topics Discussed

About Haivision™

Haivision is a global leader in delivering advanced video networking, digital signage, and IP video distribution solutions. Haivision offers complete end-to-end technology for video, graphics, and metadata to help customers build, manage and distribute their media content to users throughout an organization or across the Internet. Haivision has specific expertise in the enterprise, education, medical/healthcare, and federal/military markets.

Haivision is based in Montreal and Chicago, with technical centers in Beaverton, Oregon; Austin, Texas; and Hamburg, Germany.

Audience

This user's guide is intended primarily for users and network administrators responsible for managing streaming operations in their organization. The various procedures are divided into the following categories and identified by the intended audience.

Content	Intended Audience by Role
Touring the Interface	User and Administrators
Getting Started	User and Administrators
Working with Media Gateway	User and Administrators
Performing Admin Tasks	Administrators
Using the Console UI	Administrators

Reliability of Information

The information contained in this user's guide has been carefully checked and is believed to be entirely reliable. However, as Haivision improves the reliability, function, and design of its products, the possibility exists that this user's guide may not remain current.

If you require updated information, or any other Haivision product information, contact:

Haivision
4445 Garand
Montréal, Québec, H4R 2H9 Canada

Telephone: 1-514-334-5445
Email: infodev@haivision.com

Or visit our website at: http://www.haivision.com.

Obtaining Documentation

You can download product documentation through the Haivision Download Center at http://www.haivision.com/download-center/.

NOTE
A login is required to access the Haivision Download Center.

Service Support

Haivision is committed to providing the service support and training needed to install, manage, and use your Haivision software.

For more information regarding service programs, training courses, or for assistance with your support requirements; contact Haivision Technical Support using our Support Portal at: http://www.haivision.com/support-portal-home/.

Document Conventions

The following conventions are used throughout this document.

Typographic Conventions and Elements

Italics	Used for the introduction of new terminology or for words being used in a different context, and for placeholder or variable text.
Bold	Used for strong emphasis.
Monospaced	Used for code examples, command names, options, responses, error messages, and to indicate text that you enter.
Button	Indicates a button or some object that you click.
SMALL CAPS	Indicates a screen name or element.
>	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.

Alert Elements

The following Alert elements 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. IMPORTANT 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, or minor to moderate injury. It may also be used to alert against unsafe practices.

WARNING

Indicates an imminently hazardous situation which, if not avoided, could result in serious injury or death.

CHAPTER 1: Touring the Interface

The following content provides a product overview as well as a tour of the Media Gateway Web interface.

NOTE

To install and connect the appliance, please refer to the *Quick Start Guide* that accompanied the hardware.

Topics Discussed

Overview

Haivision's Media Gateway is a networking infrastructure product for configuring, monitoring, and managing streaming routes between encoding and decoding devices. It is designed to allow network administrators to quickly and easily configure source-to-destination and source-to-multiple-destination streaming routes, which can then be monitored and tuned for optimal performance.

Features

What's New

Version 1.4 supports supports DELL iDRAC and third-party Simple Network Management Protocol (SNMP) tools.

HLS Output

Media Gateway can be configured to convert an incoming stream to HLS (HTTP Live Streaming) format for output. HLS encryption is also supported.

Certificates

SSL certificates can be managed via the Security option in the Web interface.

Multi-site Live Streaming Support

Two or more Media Gateways can be paired with a Media Platform server and automatically configured to stream live video to multiple sites over the public Internet.

Stream Conversion

Media Gateway can convert (re-encapsulate) a given MPEG stream payload to and from SRT and TS UDP protocols. It can also generate multiple output streams from a single input. Supported sources for streams include: Makito X Encoder (SRT), Media Gateway (SRT), and Makito Classic Encoder (TS UDP). Supported streaming destinations include: Makito X Decoder (SRT or TS UDP), Media Gateway (SRT), CoolSign, Furnace, InStream, Stingray, and Mantaray (TS UDP).

NOTE
Media Gateway does not support third-party devices.

Unicast/Multicast Streaming

Media Gateway supports any combination of unicast in/out (TS over UDP, TS over RTP, or SRT) and multicast in/out (TS UDP only).

3rd Party Devices

Media Gateway supports the input of UDP MPEG Transport Streams (TS) from virtually any device, including non-Haivision encoders. Such streams can be "flipped" to TS/SRT for streaming or transport from one Media Gateway to another, and then reconverted to native UDP MPEG TS for final distribution.

Content inside a UDP MPEG TS is agnostic — it could be MPEG-2 video, H.264, HEVC, etc.; it could be a Single Program Transport Stream or Multiple Program Transport Stream. Any MPEG TS based ancillary data (e.g. multiple audio tracks, KLV, Closed Captioning, etc.) will be preserved end-to-end.

Note that the re-distribution of HLS streams originating from non-Haivision sources is not supported at this time.

Firewall Friendliness

Media Gateway makes it easy to establish inbound/outbound streams between Haivision products that are behind corporate firewalls, with minimal intervention from IT.

Encryption

Media Gateway allows you to leverage the end-to-end stream encryption (AES 128/256) component of SRT-enabled devices (see "Glossary" on page 116) including Makito X encoders and decoders as well as additional Media Gateway products.

Stream Management

Media Gateway allows you to establish, manage and monitor streaming routes based on configured sources and destinations. You can:

- Set SRT-specific source parameters (e.g., latency and passphrase).
- View real-time graph-based statistics (e.g., buffer time, actual latency, round trip time, retransmit rate, packet loss, etc.) to help with tuning SRT parameters.
- Download SRT statistics to a .cvs file.
- Enable FEC and configure traffic shaping on a destination.

Network Routing

Provisioned with two or more NICs, the Media Gateway lets you route unicast or multicast traffic from one network segment (e.g., SRT over WAN) to another network segment (e.g., TS-UDP over LAN).

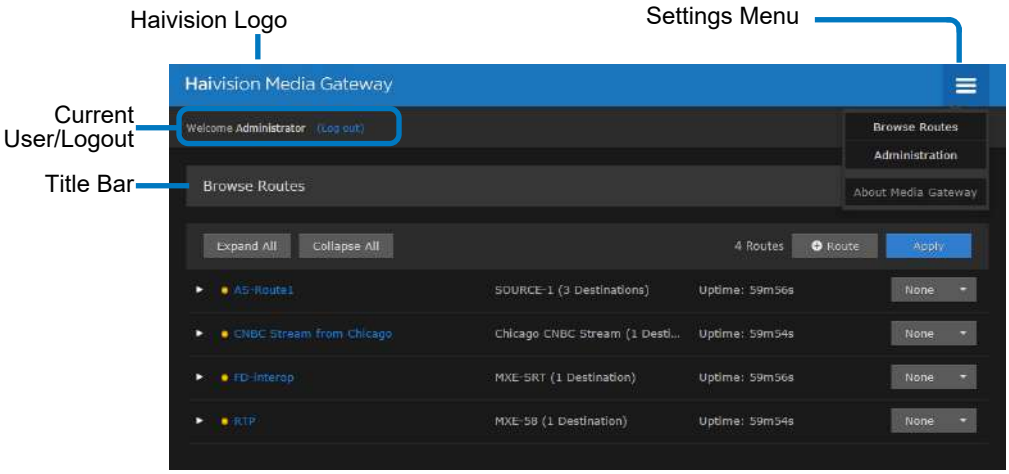
Appliance packaging

Media Gateway is available as a hardware appliance with pre-loaded operating system and software. The appliance can be easily upgraded, and has a console user interface to facilitate troubleshooting and low-level configuration.

Media Gateway is also available as a software-only product or as a cloud service (available on AWS Marketplace and Microsoft Azure).

Basic Layout and Elements

The Web interface groups device management into the following main screens: BROWSE ROUTES (home) and ADMINISTRATION. These screens use a consistent layout with common screen elements to simplify your experience.



Persistent Screen Elements

The following elements are constant and available from any screen.

Haivision Logo (Home Screen/Quick Access)

Clicking the Haivision logo at the top left of any screen takes you to the BROWSE ROUTES (Home) screen.

Settings Menu

You access the SETTINGS menu by clicking the  icon on the toolbar at the top right of every screen. The SETTINGS menu provides access to:

Browse Routes screen	Allows you create and manage routes and their source/destination nodes.
Administration screen	Provides access to system configuration tasks (e.g., status, licensing, updating, and network configuration) and user administration.
About Media Gateway dialog	Opens a dialog that displays the version number, build number, and copyright statement.

TIP

When requesting assistance, be sure to provide the build number displayed in the About Media Gateway dialog to the support representative.

Current User/Logout

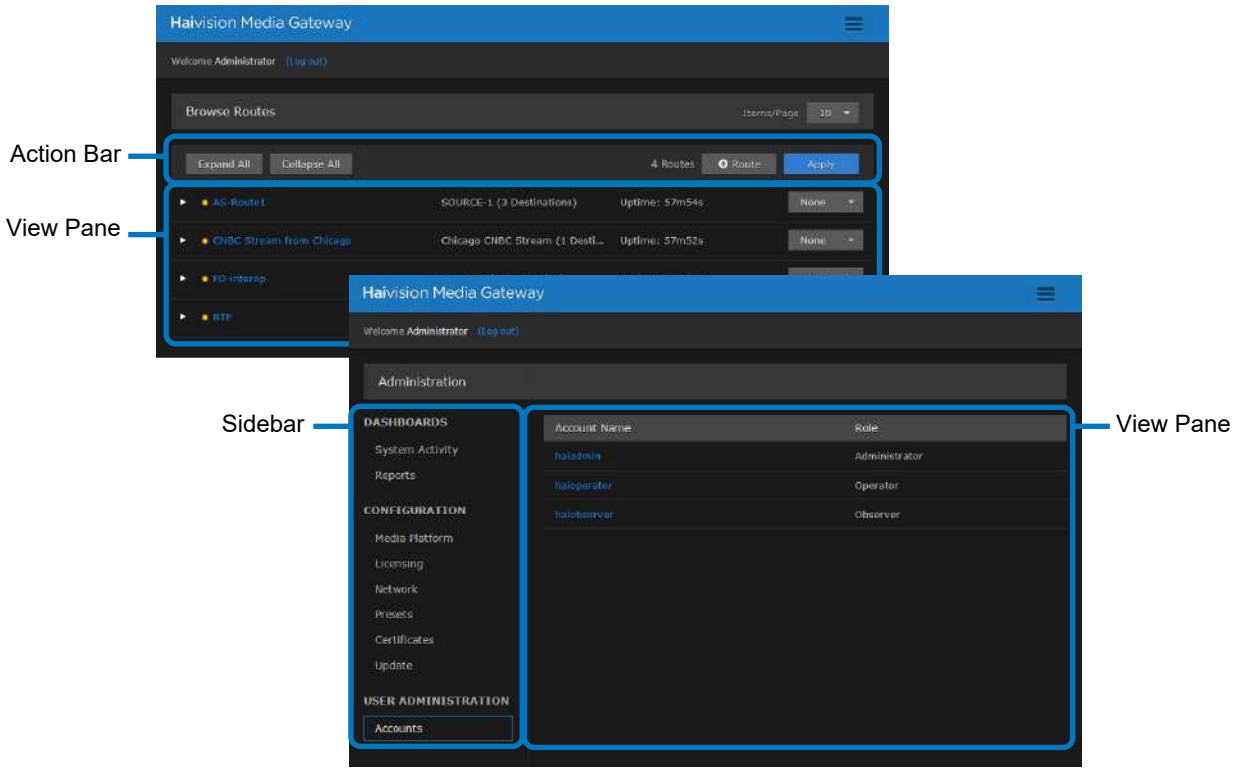
Identifies the user who is currently logged into the system. The LOG OUT action link allows you to exit out of the system and return to the LOG IN screen.

Title Bar

Identifies the name of the current screen.

Variable Screen Elements

The actual content and/or context for the following elements varies, or is contingent upon, the currently displayed screen.

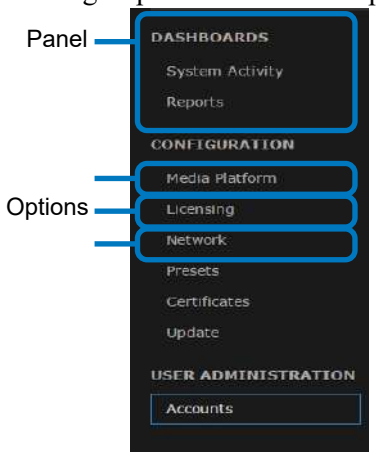


Action Bar

Depending upon the current screen, the action bar provides quick action buttons for the tasks available. Tasks are performed on all items listed in the view pane.

Sidebar

Depending upon the current screen, the sidebar provides a means to navigate various options. Related options are grouped under different panels.



View Pane

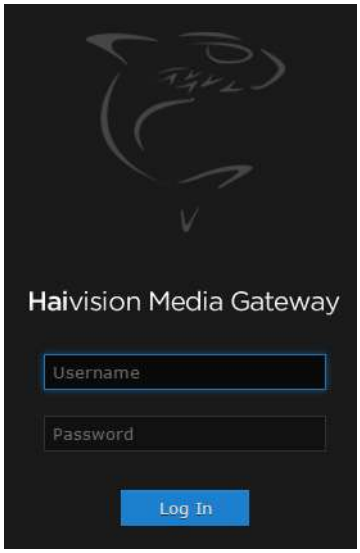
The view pane, depending on the current screen, displays the appropriate items, fields, or status information.

Interface Screens

There are several main screens that you use when working with Media Gateway.

Log In Screen

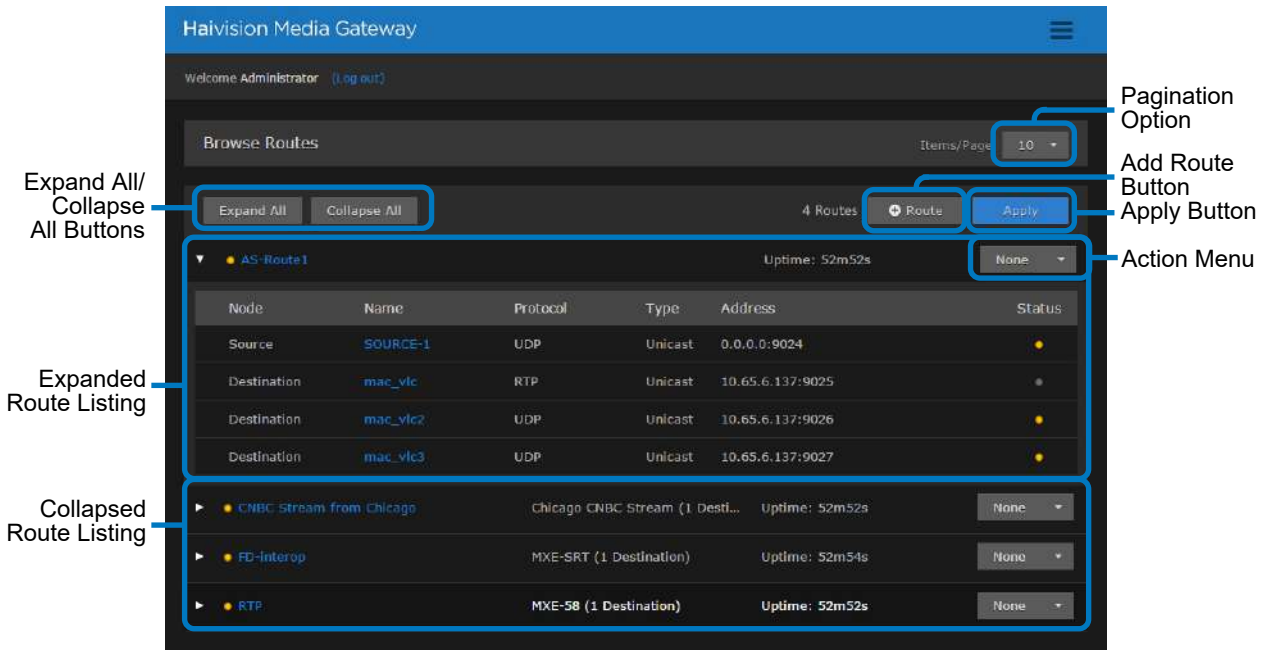
When you start the Media Gateway interface, a LOG IN screen appears prompting you to log into the system ("Logging into the Media Gateway Interface" on page 24).



Once you log in, the Browse Routes screen is displayed.

Browse Routes Screen

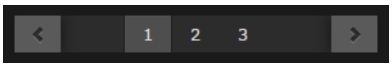
The BROWSE ROUTES screen gives you a quick overview of the devices currently managed by Media Gateway. The View Pane lists the available routes. You can expand/collapse the routes to list more detailed information regarding their source and destinations.



Browse Routes Screen Elements

Title Bar

The Title Bar includes a drop-down menu to select how many routes to show per page. If the number of defined routes is greater than this setting, then page controls are available below the route listing. For example:



Action Bar

The Action Bar contains the following buttons:

- Expand All / Collapse All — Expands/Collapses the details of all routes, including: node, name, protocol, address, type, and status.
- +Route — Click to add a new route. See "Creating a Route" on page 45.
- Apply — Used to apply multiple routes' drop-down menu selections at one time.

View Pane

The view pane includes a listing of all configured routes. It includes the following for each route when the routes are either expanded or collapsed:

- ▶ / ▼ — Click to expand or collapse the route details.
- **Status**
  - ● — Active with data flow
  - ● — Active with no data flow
  - ● — Error
  - ● — Inactive
- **Route Name** — Provides the route's name (limited to 128 characters). Click to open the EDIT ROUTE screen.
- **Source Name** — (Only shown when route is collapsed.) Provides the name of the route's source (limited to 128 characters). The number of destinations is also shown in parantheses next to the source name. Click to open the EDIT ROUTE screen.
- **Route Uptime** — Displays how long the route has been active. Click to open the EDIT ROUTE screen.
- **Action Menu** — Drop-down menu that offers selections for None, Start, Stop, and Delete. A spinning icon is displayed next to the route name if the route has pending updates. While the update is pending, you cannot edit the route or any of its source/destinations.

View Pane (Expanded)

Lists the routes along with *source* and *destination* information in the view pane. Information provided includes:

- **Node** — Indicates whether the listing is a source or destination for the route.
- **Name** — Provides the node's name (limited to 128 characters).
- **Protocol** — Indicates the streaming protocol being used by the node.
- **Type** — Identifies the stream type, such as Multicast or Unicast.
- **Address** — Displays the address for the node.
- **Status** — Provides a status indicator for each device and the length of time since the device has been actively connected. Connection status indicator states include:
  - ● — Active with data flow
  - ● — Active with no data flow
  - ● — Error

- ● — Inactive

NOTE

Hovering over the indicator in the STATUS column opens a tooltip with more details (for example, recent connection information, various thresholds being met, or errors, such as “stream stops” and “video feed gets disconnected”).

Related Topics

- “Working with Media Gateway” on page 28

Administration Screen

The ADMINISTRATION screen allows you to connect to, manage, or add new devices.

The sidebar at the left lists the available actions. The currently selected action is indicated with a blue hover highlight on the left side of the button. The view pane displays the appropriate fields or items for your chosen selection. Likewise, selections made in the view pane may also alter the available fields or options in the view pane.

To navigate to the ADMINISTRATION screen, click the  icon on the toolbar and click **Administration** from the drop-down menu.

Administration Screen Elements

Sidebar

The sidebar groups the options into various panels:

- DASHBOARDS PANEL
  - **System Activity** — Provides quick statistics on the system (CPU/memory usage and system uptime), the current version of the software, Video-on-Demand (VOD) bandwidth graph, and disk space statistics.
  - **Reports** — Offers access to a number of different logs providing system, application, and diagnostic messages.
- CONFIGURATION PANEL
  - **Media Platform** — Provides the status and settings pane for pairing the Media Gateway with a Media Platform.
  - **Licensing** — Allows you to add Media Gateway licenses and view their bandwidth limits and status.
  - **Network** — Provides access to the network configuration settings as well as information on the interfaces.
  - **Presets** — Allows you to export the current configuration as a preset file and import a preset file and apply it to the device.

- **Security** — Allows you to install an SSL security certificate.
- **Update** — Identifies the currently installed bundle and allows you to update to a new version of software.

- USER ADMINISTRATION PANEL
  - **Accounts** — Identifies the current roles (administrator, operator, and observer) on the system and the members for each. Allows you to change the user passwords.

View Pane

Displays the appropriate content based on the current selection in the sidebar.

Related Topics

- "Performing Admin Tasks" on page 61

About Media Gateway Dialog

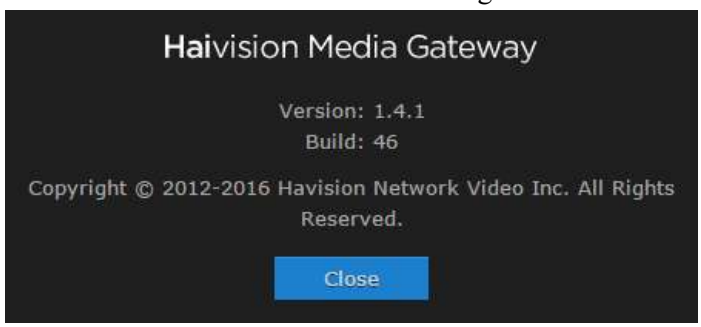
The ABOUT MEDIA GATEWAY dialog provides you with information regarding the current version and build of the installed product and the copyright information.

To open the About Media Gateway dialog:

1. Click the  icon on the toolbar.
2. Click **About Media Gateway** from the drop-down menu.

To dismiss the About Media Gateway dialog:

1. Click the Close button to dismiss the dialog.



CHAPTER 2: Getting Started

The following content explains how to access and log into the Media Gateway.

NOTE

Before proceeding, make sure that the system is set up correctly and a network connection is established as detailed in the *Quick Start Guide*. Contact your system administrator for assistance with network configuration.

Topics Discussed

Accessing Media Gateway

To access the interface, perform the following procedures for logging into and out of Media Gateway.

NOTE
Reference the *Important Notice* document or contact your system administrator for login credentials.

Logging into the Media Gateway Interface

NOTE
To log into Media Gateway, ensure that your browser has cookies enabled.

To access the Media Gateway:

1. Open a Web browser and enter the URL or IP address of the Media Gateway server in the browser's address bar. For instance:

   http://<ipaddress>/ or

   http://<system url>/

   where:

   - <ipaddress> is the IP address of the system where Media Gateway is installed. For example, http://10.69.12.152. Connect a monitor to the appliance to display this address on the Console UI. For details, see the *Quick Start Guide*.
   - <system url> is the system's URL, such as http://gateway.haivision.com.

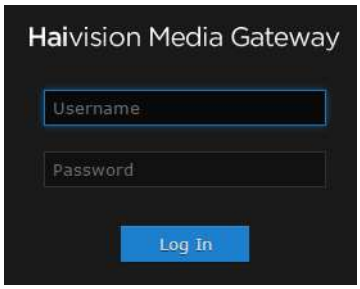
2. When the browser accesses the Media Gateway website, it requests the security certificate to confirm that the site is trusted. If a security certificate is not available or is self-signed, a message similar to the following appears. See "Media Gateway SSL Encryption" on page 25 for more details.

NOTE
Responses may vary depending upon the browser used.

IMPORTANT

Before proceeding or adding an exception for the site, check with your administrator on the correct response.

3. At the LOG IN screen, enter your Media Gateway username and password. See the Important Notice document for these credentials and more information.



4. Click the Log In button. The Web interface opens to the BROWSE ROUTES screen.

Related Topics

- "Log In Screen" on page 18
- "Logging Out of the Media Gateway Interface" on page 27
- "Media Gateway SSL Encryption" on page 25
- "Changing an Account's Password" on page 95

Media Gateway SSL Encryption

Media Gateway is encrypted to provide secure interactions with your devices. When you log into the Media Gateway 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.

NOTE
The security certificate is stored at /opt/haivision/madra/conf/nginx/server.crt

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

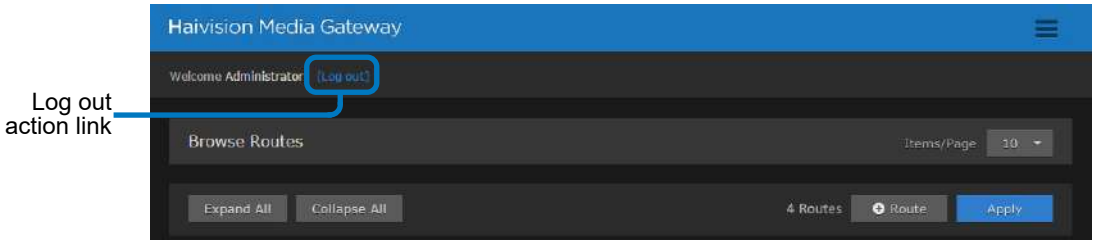
Supplying the Media Gateway with an SSL security certificate eliminates the security warning, provides a means for users to verify a website, and ensures that the connection is secure. See “Certificates” on page 86 for more details.

Related Topics

- “Certificates” on page 86

Logging Out of the Media Gateway Interface

1. When logged into the Media Gateway Interface, click the Log Out action link at the top left corner of any screen to log out.



NOTE

If there is no activity over a period of ~2 minutes, the system automatically logs you out of the session.

Related Topics

- "Persistent Screen Elements" on page 15
- "Logging into the Media Gateway Interface" on page 24

Changing Passwords

IMPORTANT

For security purposes, change the password for each of the available accounts. Information regarding user/password credentials should be safe-guarded. See "Changing an Account's Password" on page 95 for details of changing passwords.

Factory-set passwords are provided in the *Important Notice* document.

CHAPTER 3: Working with Media Gateway

The following content provides a Media Gateway overview and discusses how to work with routes.

Topics Discussed

Overview

Media Gateway enhances your Haivision ecosystem's infrastructure to simplify the distribution of live video/audio across multiple facilities, while maintaining bandwidth efficiency at each of the locations.

Once in place, Media Gateway allows network administrators to quickly and easily configure source-to-multiple-destination streaming *routes*, which can then be monitored and tuned for optimal performance.

One of the most popular uses for Media Gateway is to distribute a live video/audio stream across multiple facilities to a variety of devices. This might be done to stream a quarterly all-hands meeting to remote sites, a class to remote campuses, and so forth.

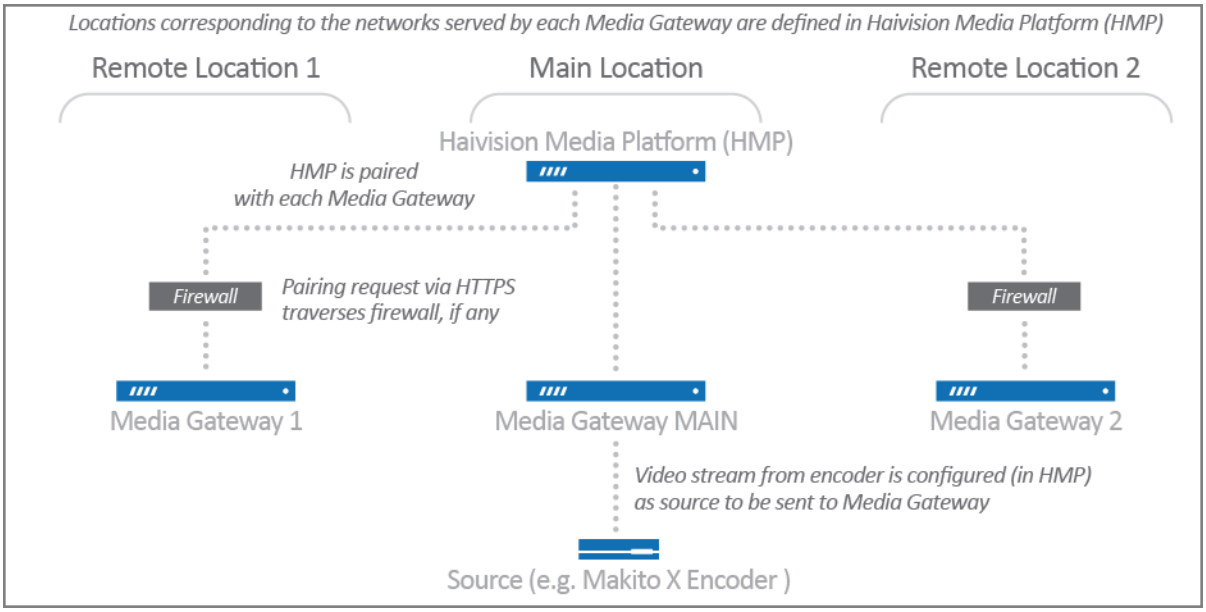
While MPEG-based streams typically do not fare well traveling across the internet, the latest Haivision SRT protocol easily optimizes streaming over unpredictable networks, ensures end-to-end security, and traverses firewalls. Plus, Media Gateway allows stream conversion to TS over UDP or TS over RTP, so you can utilize SRT technology with your existing/older devices (even those not inherently SRT-capable).

Multi-site Live Workflow

As of Version 1.2, Media Gateway works with Media Platform (Version 2.1 or higher) to support live video distribution across a multi-site environment. This capability leverages Haivision's SRT technology to transport the video over lossy networks such as the public internet, and to easily traverse firewalls.

Pairing the Gateways with Media Platform

The first step in establishing a multi-site live configuration is to pair the Media Gateways with the Media Platform that is driving the session:



In Media Platform, you also need to establish a connection between the video source (for example, a Makito X Encoder) and one of the paired Media Gateways.

NOTE

The video source can be connected to the Media Gateway at any of the locations. It does not have to be co-located with the Media Platform. The Media Gateway to which the source is connected must, however, be identified as such on the Media Platform.

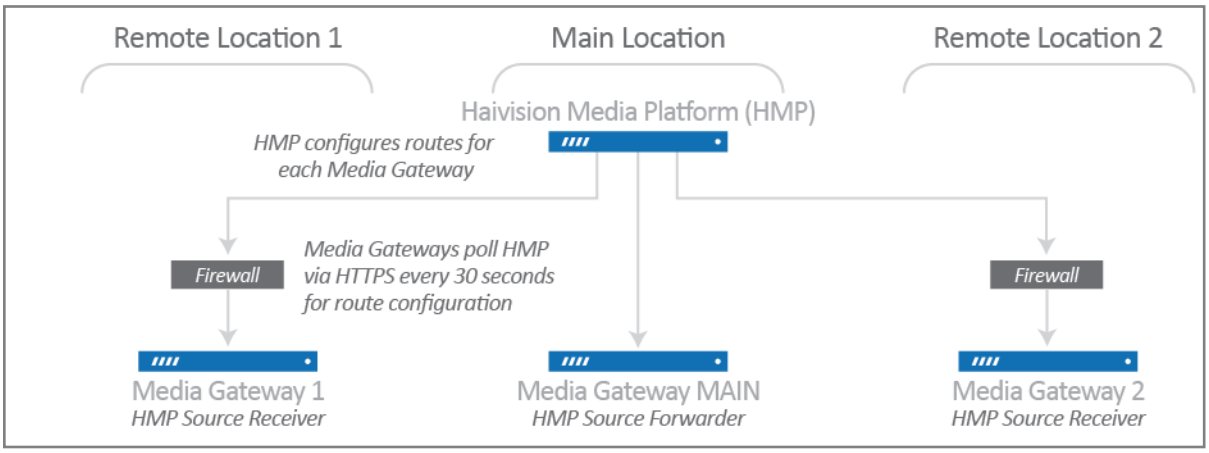
Defining the Locations (Media Platform)

After the pairings are complete, you define "locations" in the Media Platform corresponding to the networks served by the various Media Gateways (i.e., the networks on which the users watch the live video). The Media Gateway serving as the ingest point for the live video is considered to be the **source forwarder** in this context. The other Media Gateways are identified as **source receivers**. Based on these locations and the forwarder/receiver designations, Media Platform generates routing configurations for each

of the locations. The respective Media Gateways poll the Media Platform at intervals of approximately 30 seconds, and download the routing configuration files.

NOTE

If you modify a multi-site live route on any of the associated Media Gateways, it is eventually overwritten by the original configuration from Media Platform.



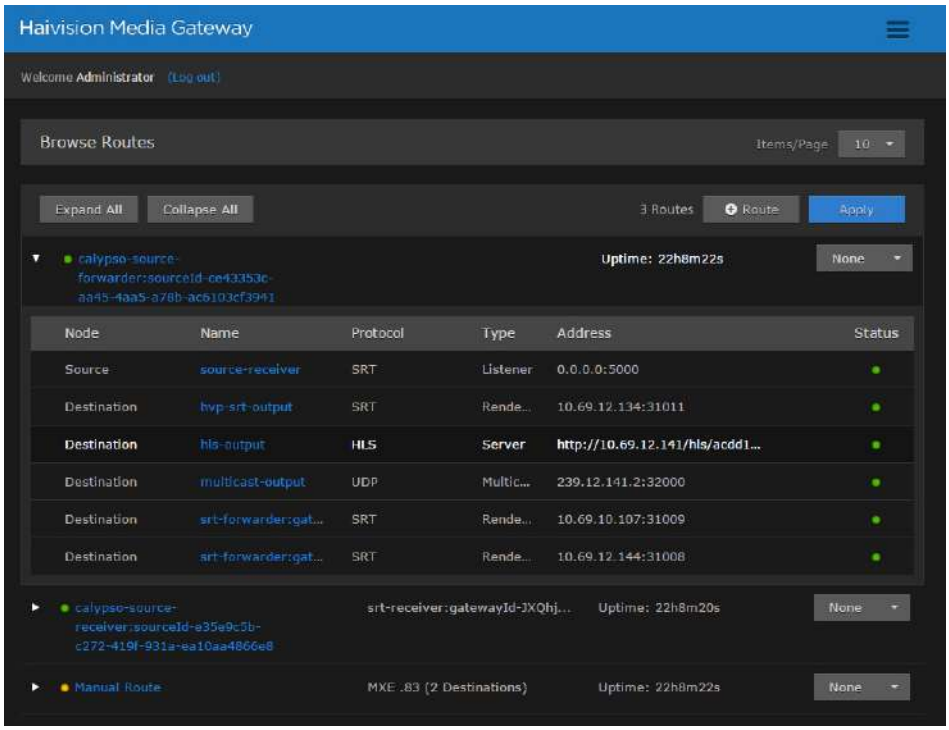
Source Forwarder

For the Media Gateway to which the video source is connected (the forwarder), Media Platform creates a route consisting of one source and multiple destinations. The route is identified by a name with the following syntax:

```
calypso-source-forwarder:sourceId-[ID]
```

A route with this name indicates that the Media Gateway is receiving traffic from a source (e.g., a Makito X Encoder) and forwarding it to Media Platform. The source ID corresponds to the ID of the source.

In the following sample screenshot, the route shows the Media Gateway (forwarder) propagates the source to four destinations: one corresponding to an HLS stream for the local audience, two for "forwarding" the live video to remote Media Gateways via SRT, and one SRT Listener. The SRT Listener destination allows Media Platform to connect as an SRT Caller to access the video for recording:



NOTE

The status of the SRT Listener destination may intermittently change from green to yellow and back, because the Media Platform only establishes a connection as needed.

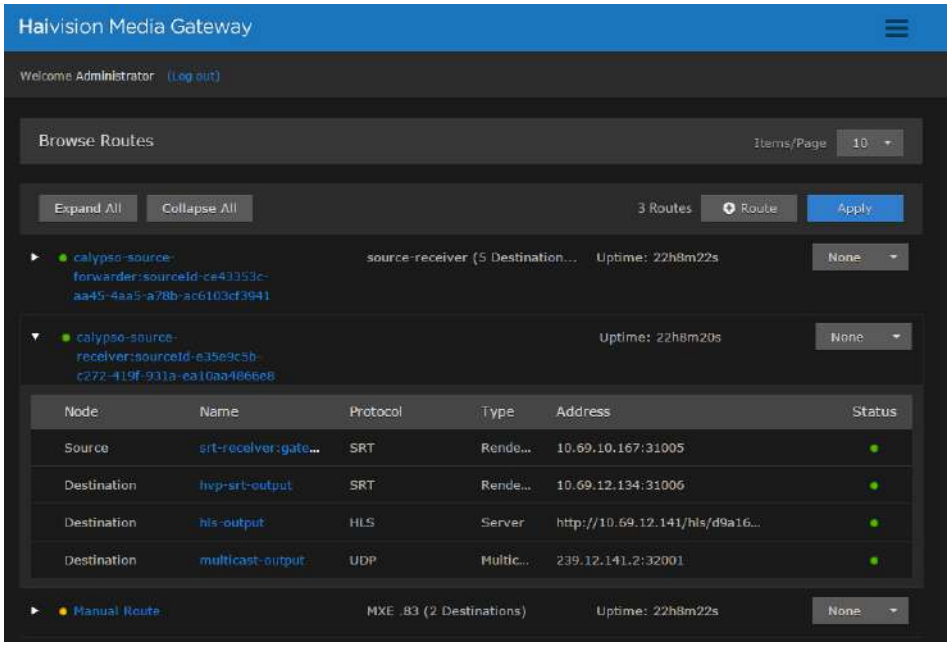
Source Receivers

For each Media Gateway (receiver) to which the live video is being sent, Media Platform creates a route consisting of one source and one destination. The route is identified by a name with the following syntax:

```
calypso-source-receiver:sourceId-[ID]
```

A route with this name indicates that the Media Gateway is receiving traffic from another Media Gateway (the forwarder) for local output. The source ID corresponds to the ID of the live video source.

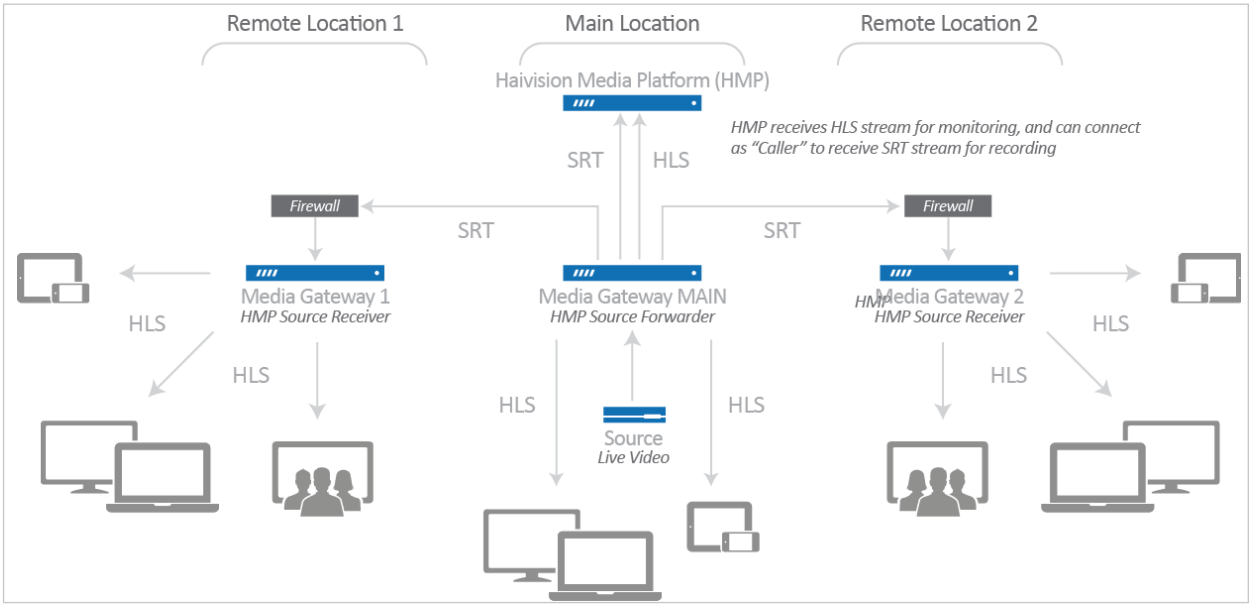
In the following sample screenshot, the route shows the Media Gateway (receiver) propagates the source to a single destination, corresponding to an HLS stream for the local audience:



NOTE

If someone copies the HLS Destination URL and tries to view the video in a browser, they get an authentication error. Viewers must be authorized through Media Platform.

2. After the live session is initiated, the video automatically streams to and is viewable by the audience at all locations (as shown in the following diagram):

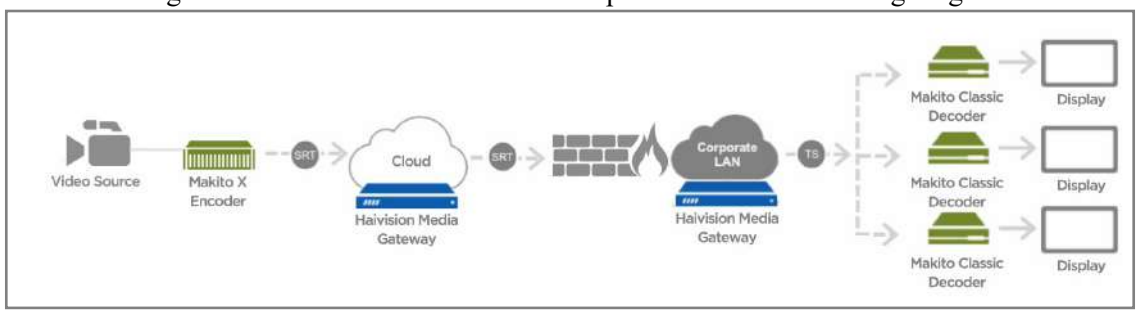


For more information, including complete instructions on how to configure a multi-site live session, please refer to the *Haivision Media Platform Administration Guide*.

Multicast Workflow

The following workflow steps you through an encoder sending an SRT stream to a hosted instance of Media Gateway on the cloud, which routes each destination segment. At the remote sites, a Media Gateway (on the corporate LAN) converts the SRT protocol to a format compatible with the local viewing devices.

A general overview of this workflow is provided in the following diagram:



In the above diagram, the cloud-based Media Gateway (located on the Public Internet or as a Haivision Video Cloud (HVC) hosted option) is *optional* and only recommended for individuals who want to "own" the distribution or have concerns about low latency. A Media Gateway can also be hosted on the LAN to allow multi-sites distribution.

NOTE

The various receivers are not always SRT-capable, but Media Gateway can accept inbound SRT streams and flip these streams into a format compatible with internal receivers.

Run-Through Example

TIP

You'll find some helpful videos on our website that show you how this is done. Check out http://www.haivision.com/ for more information.

Before stepping through this example, you need to have the Media Gateway installations available in the cloud and on your local area network.

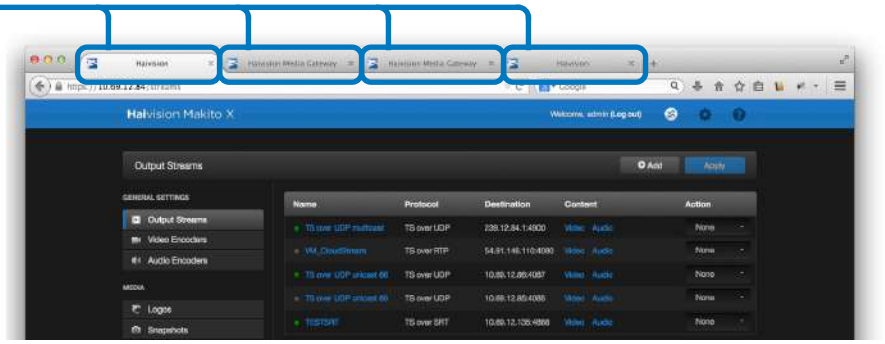
TIP

Use the tabs in one browser to point to the URL of each workflow element to create a workspace. For example, access the Makito X web interface of your source on one tab, the cloud Media Gateway on another, and so forth. This way, you can switch back and forth between them.

Creating your Workspace *(Optional)*

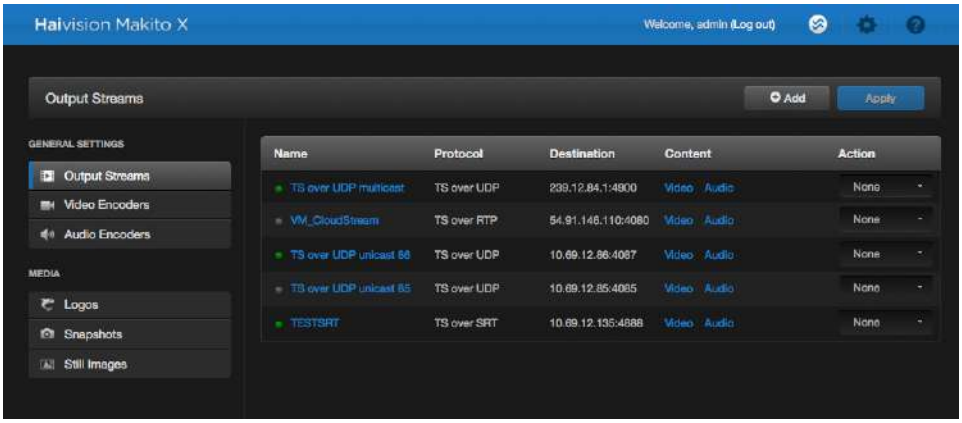
1. In your web browser, open a tab, enter the Makito X Encoder web interface URL, and log in when prompted.
2. Open another new tab, enter the cloud-based Media Gateway web interface URL, and log in when prompted.
3. Open another new tab, enter the remote site's LAN-based Media Gateway web interface URL, and log in when prompted.
4. Open another new tab, enter the Makito X Decoder web interface URL, and log in when prompted.

Open a tab for each device that you are connecting.



Establishing the Source

1. If you followed the steps in "Creating your Workspace (Optional)" on page 36, switch to the Makito X Encoder's browser tab. Else, enter the URL for the Makito X encoder web interface and log in when prompted.
2. On the Makito X Encoder's navigation sidebar, click Output Streams.

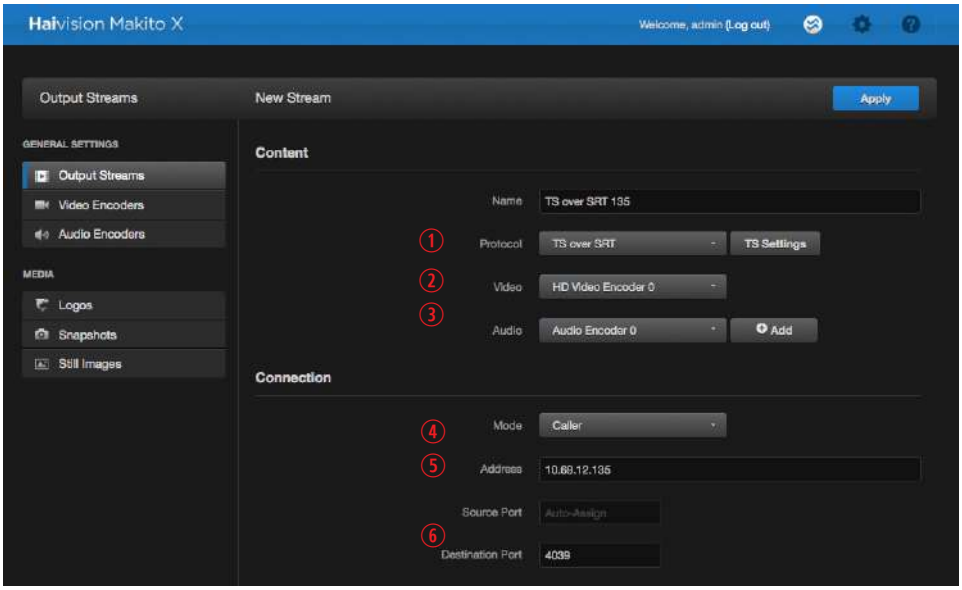


3. The view pane lists the available streams. For this example, we are going to add a stream that uses TS over SRT. Click the +Add button. *If you have an existing SRT stream, you can modify it instead.*

NOTE

Refer to your Makito X documentation for more information on adding streams if you are new to this process.

4. When the NEW STREAM screen opens, provide a ① stream name and specify the ② TS Over SRT protocol. For ③ video, select an active video encoder.



5. Under the Connection section, specify the ④ mode as "Caller," enter the ⑤ address for the Media Gateway (in the Cloud) and a ⑥ Destination port.

TIP

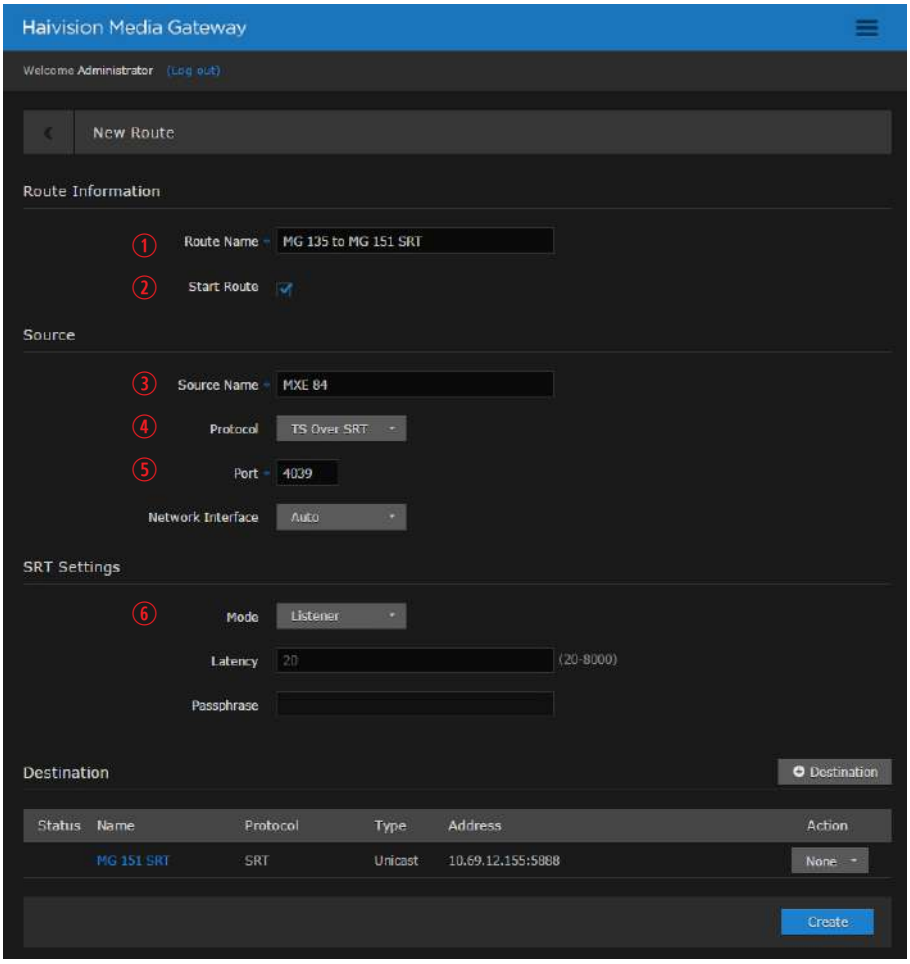
If needed, switch to the appropriate browser tab or enter the URL for the cloud-hosted Media Gateway to acquire this information.

6. Click Apply.

Connecting the Source to the Cloud-Hosted Media Gateway

1. If you followed the steps in "Creating your Workspace (Optional)" on page 36, switch to the Media Gateway's browser tab. Else, enter the URL for the Media Gateway encoder web interface and log in when prompted.
2. On the BROWSE ROUTES screen, click the +Route button.

3. When the New Route screen opens:
   - In the Route Information section, supply a ① route name and click the ② Start Route checkbox so that the stream is started after creation.
   - In the Source section, provide a ③ source name, specify the ④ protocol as TS Over SRT (for this example), and enter the ⑤ port from the source encoder.
   - In the SRT Settings section set the ⑥ mode to Listener.

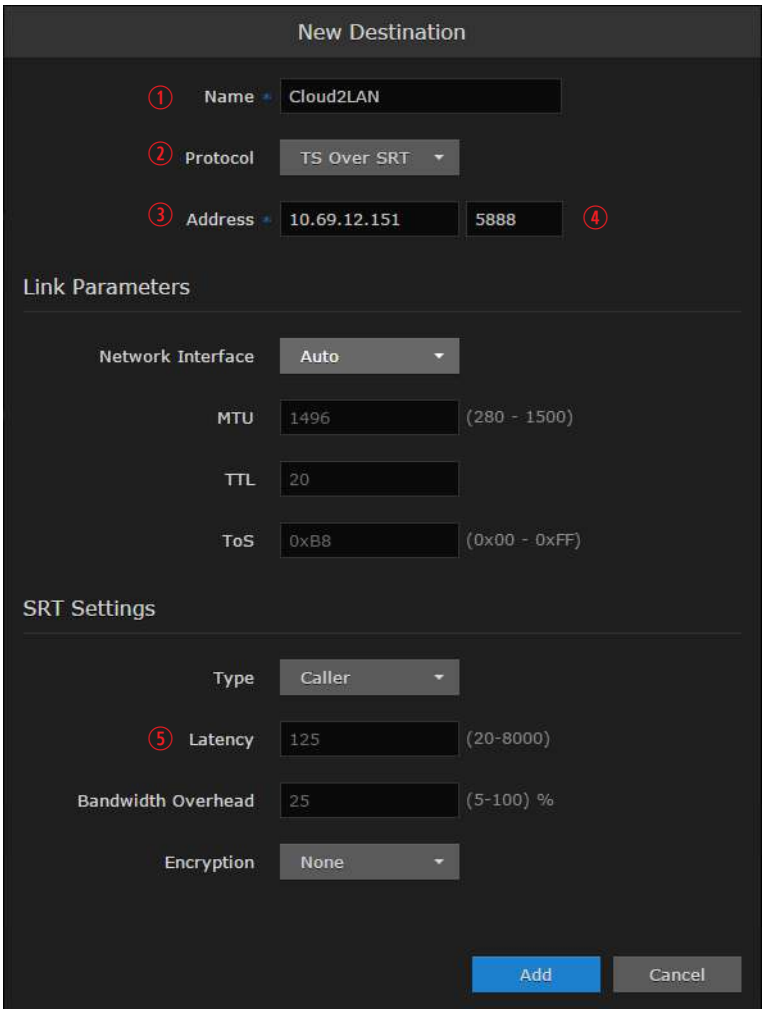


TIP

If needed, switch to the Makito X Encoder browser tab or enter the URL for the Makito X Encoder to acquire this information.

4. Click the +Destination button.
5. In the New Destination dialog:
   - Change the ② protocol to "TS over SRT."
   - Under the SRT Settings section, change the ⑤ type to "Caller."

- Enter the information for the LAN-based Media Gateway. Provide a ① name, the ③ address, and the ④ port information.



NOTE

Protocols and types can have different configuration requirements. Data fields will appear or disappear depending upon your choices. As just demonstrated, SRT protocols require an address, in addition to a port, when they are running in Caller type.

TIP

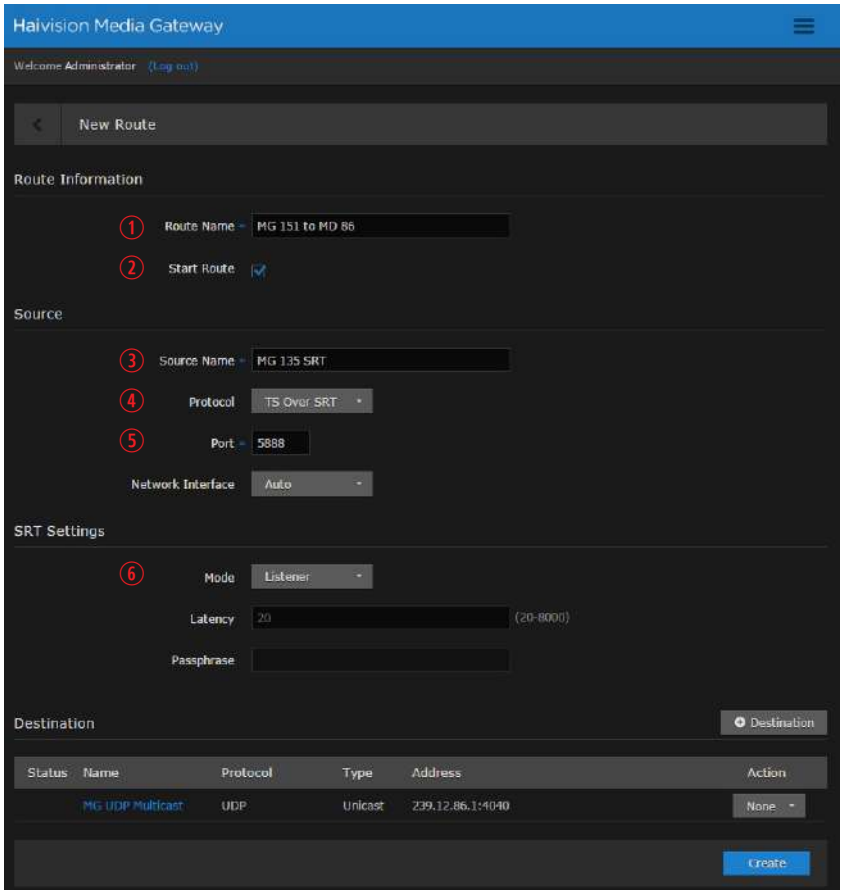
If needed, switch to the LAN-based Media Gateway browser tab or enter the URL for the LAN-based Media Gateway to acquire this information.

6. When finished, click Add.
7. On the New Route screen, when finished, click Create.

8. On the BROWSE ROUTES screen, expand the route to verify that the status lights change to green.

Connecting the Media Gateway to the Remote Site's Makito X Decoder

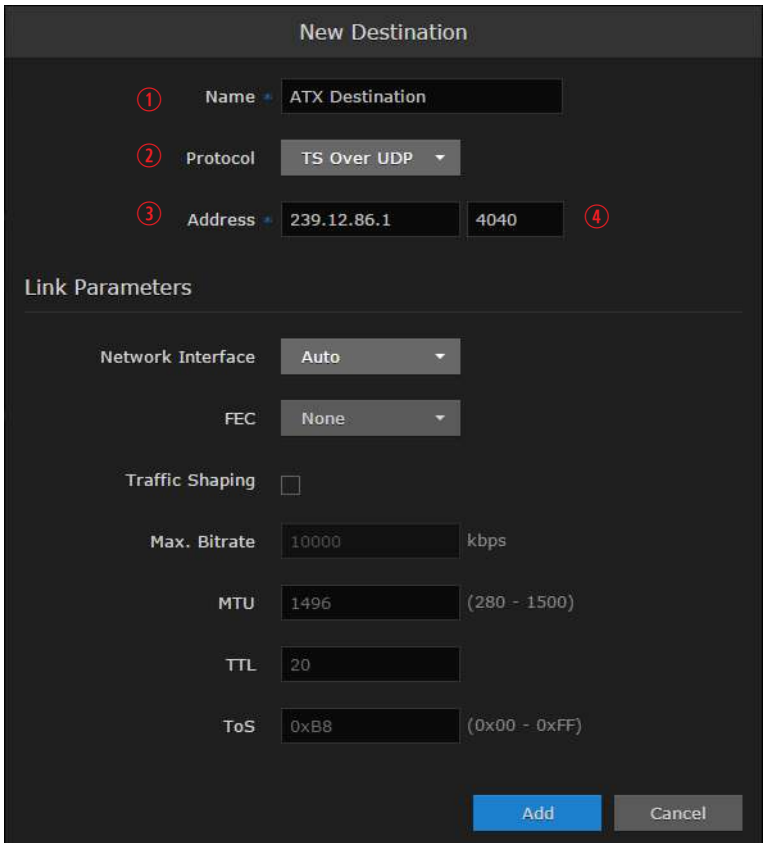
1. Switch to the LAN-based Media Gateway browser tab or enter the URL for the LAN-based Media Gateway web interface.
2. Click +Route button to add a new route.
3. In the New Route screen:
   - Supply a ① route name and click the ② Start Route checkbox so that the stream will be started upon creation.
   - In the SOURCE section, provide a ③ source name, the ④ protocol, and ⑤ port.
   - Set the ⑥ mode to "Listener" under the SRT Settings section.



TIP

If needed, switch to the appropriate browser tab or enter the URL for the LAN-based Media Gateway to acquire this information.

4. Click +Destination.
5. In the NEW DESTINATION dialog:
   - Enter the information for the Decoder. Provide a ① name and the ② protocol.
   - In this example, we are using a protocol of TS over UDP so you also add the ③ Multicast address and ④ port information.



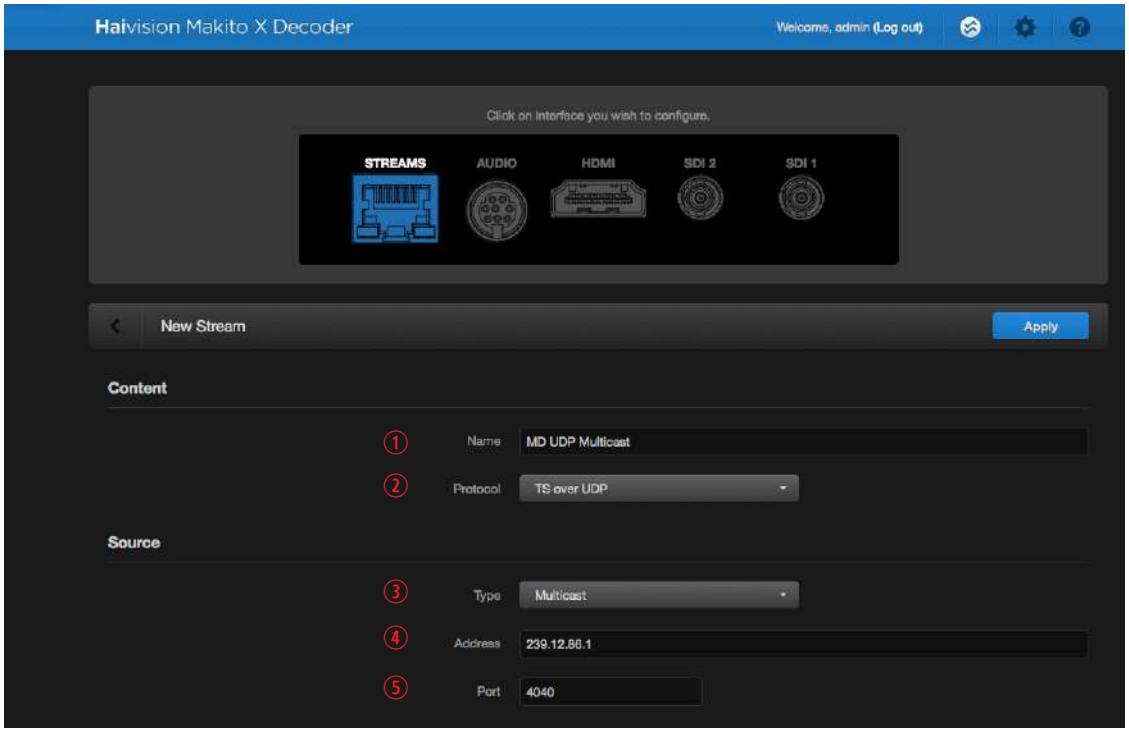
6. When finished, click Add.
7. In the New Route screen, click Create.

Connecting the Makito X Decoder

1. Switch to the Makito X Decoder tab or enter the URL for the Makito X Decoder web interface.
2. Click +Add to add the stream to the Makito X Decoder.
3. On the NEW STREAM screen:
   - Enter a ① name and the ② protocol.

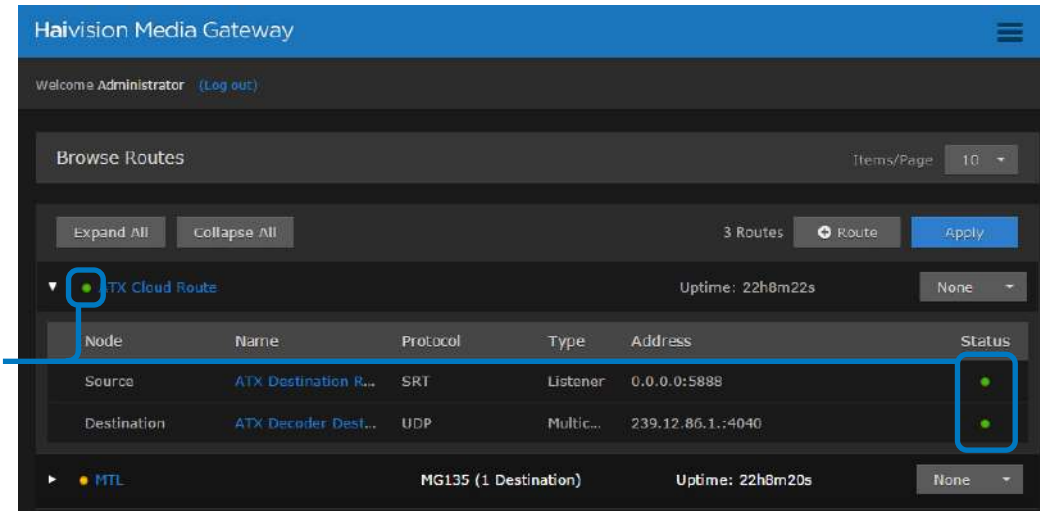
- For this example, we are flipping the stream to multicast TS over UDP to accommodate older Makito X Decoders. So, you need to include the ③ type ④ address and ⑤ port information.

NOTE
Multicast addresses are in the range of 224.0.0.0 to 239.255.255.255.



4. Click Apply.
5. Repeat steps #2 and #3 as needed to define additional streams.

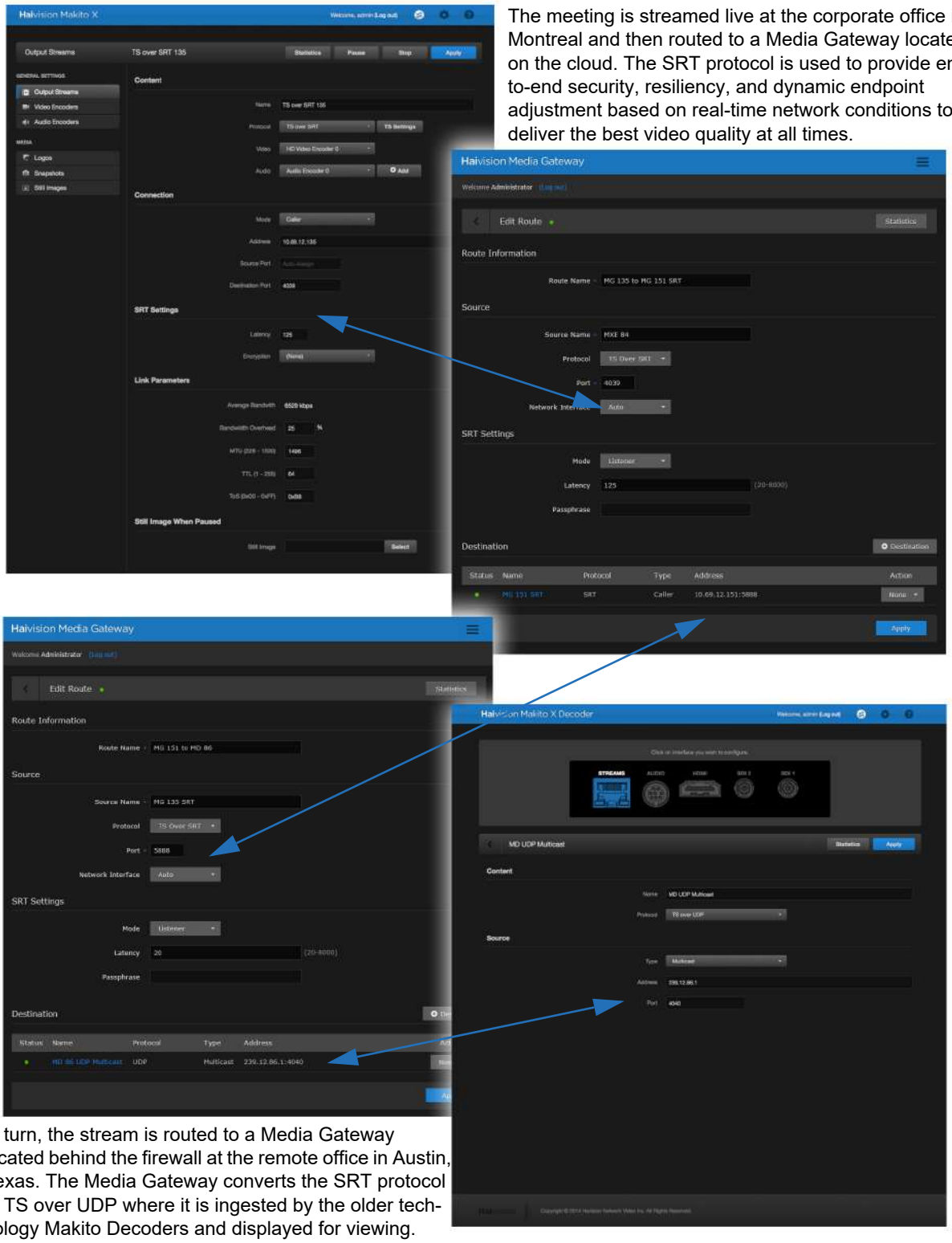
6. To ensure that everything is set up properly, verify that the stream(s) have green status indicators.



NOTE

Refer to your Makito X Decoder documentation for more information on displaying streams.

Run-Through Example Recap



The meeting is streamed live at the corporate office in Montreal and then routed to a Media Gateway located on the cloud. The SRT protocol is used to provide end-to-end security, resiliency, and dynamic endpoint adjustment based on real-time network conditions to deliver the best video quality at all times.

In turn, the stream is routed to a Media Gateway located behind the firewall at the remote office in Austin, Texas. The Media Gateway converts the SRT protocol to TS over UDP where it is ingested by the older technology Makito Decoders and displayed for viewing.

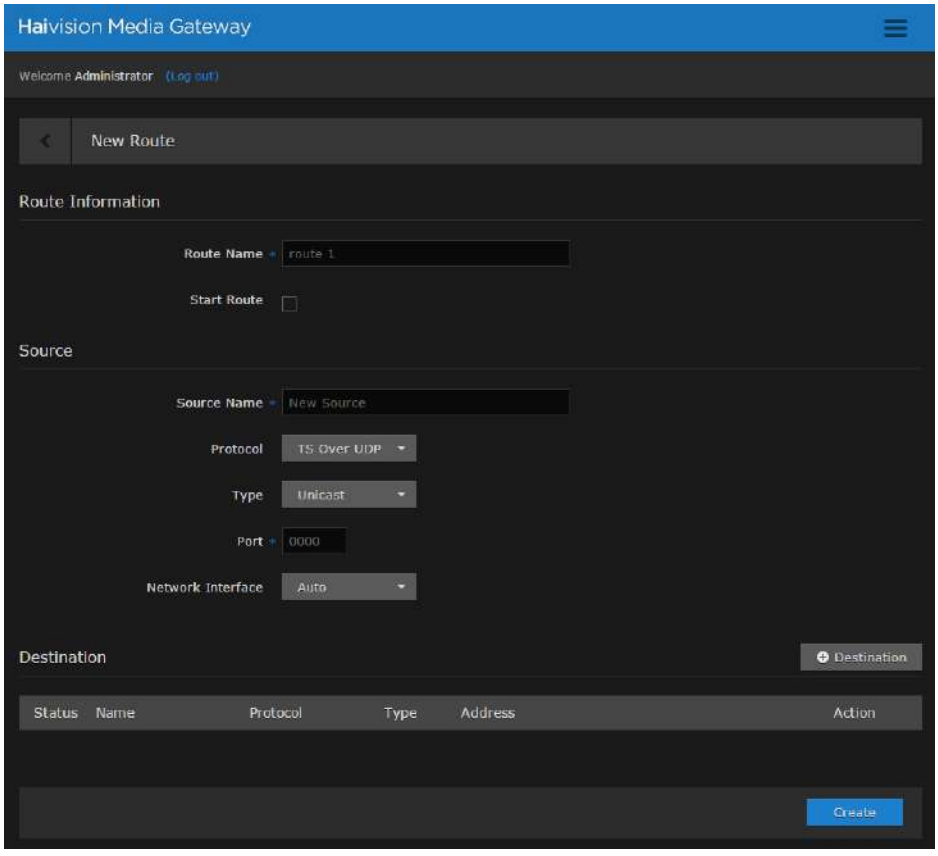
Working with Routes

NOTE
Be careful with running routes. Any of the following actions, when applied, override all the destination states.

Creating a Route

To create a route:

1. Click the icon and click Browse Routes.
2. On the Actions bar, click the +Route button.
3. On the NEW ROUTE screen, provide appropriate settings for the route. The required fields are identified with a blue asterisk. Explanations for the fields are provided in "Available Route Settings" on page 48.



Route Information

Enter the Route Name. If you want the route to be active as soon as it is created, click the Start Route checkbox.

Source

A source is a live incoming transport stream. In this section you identify the encoding device. After you have provided a Source Name, use the drop-down menu to select the streaming Protocol. Depending upon your choice, additional fields appear:

- **TS Over UDP** and **TS Over RTP** — For these protocols, choose the stream type:
  - For **Unicast**, supply the Port of the source.
  - For **Multicast**, supply the Address and Port of the source. NOTE: Multicast addresses are in the range 224.0.0.0 through 239.255.255.255.
- **TS Over SRT** — For this protocol, supply the port of the source. Selecting TS Over SRT, opens an additional SRT Settings section.

SRT Settings

(Only for TS Over SRT protocols.) Specify the Mode:

- **Caller** — Actively initiates a connection the call request.
- **Listener** — Passively waits to receive a connection call request.
- **Rendezvous** — A special case where both source and destination try to initiate the connection, while at the same time wait to receive a connection request from the peer.

NOTE

If *Caller* or *Rendezvous* is chosen for Mode in the SRT Settings section, an Address field is prefixed to the Port field in the Source section.

IMPORTANT

If *Encryption* is being used on the SRT stream, you must set the same passphrase as is used in the encoder.

Destination

Each route can contain no or multiple destinations. This section allows you to add and edit destinations, as well as perform actions, including start and stop destinations.

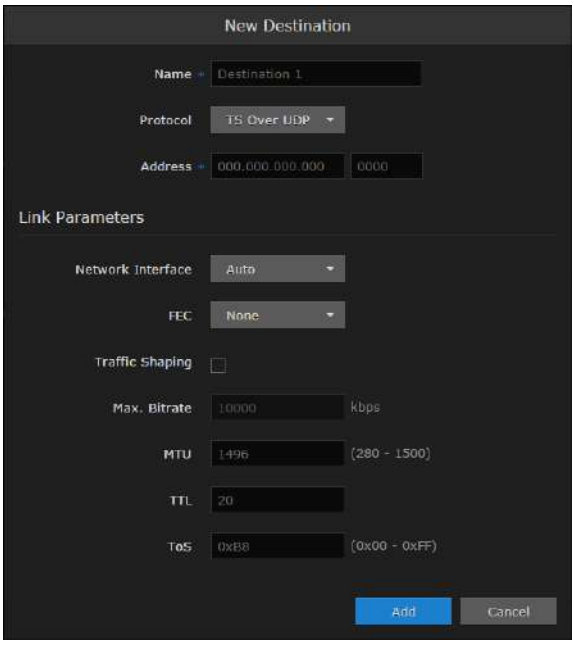
- **Add Destination** — Click the +Destination button to open a New Destination dialog; enter all required fields and click Apply. The destination is added to the list.

- **Edit Destination** — Click on a destination row to open the Edit Destination dialog for the selected destination; make changes and click Apply. The changed value is displayed in the list;
- **Destination Actions** — Click on a destination row, click on an action (such as Start, Stop, or Delete).

IMPORTANT

Destination operations (add, edit, and actions), are not saved to the server until the Apply or Create button is clicked on the ROUTE page.

4. To add the Destination, click the +Destination button at the bottom of the screen.
5. When the NEW DESTINATION dialog opens, provide appropriate settings for the Destination. The required fields are identified with a blue asterisk. For information on the various fields, see *"Destinations"* on page 49.



6. Checking the Traffic Shaping checkbox allows you to manually adjust the maximum bitrate. Traffic Shaping controls the outgoing stream so that the inter-packet time is constrained, in order to reduce the probability that TCP packets are dropped in a session.

   Enabling Traffic Shaping does *not* dynamically modify the video encoder bitrate.

Available Route Settings

Route Setting	Description
Route Information	
Route Name[1]	Name (limited to 60 printable characters). TIP: Keep the name under 18 characters to have the entire name displayed in the Browse Routes screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.
Start Route	Check this box to start the route upon creation.
Source	
Source Name[1]	Name (limited to 60 printable characters). TIP: Keep the name under 18 characters to have the entire name displayed in the Browse Routes screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.
Protocol	Select from the drop-down menu one of the available streaming protocols: • TS Over UDP • TS Over SRT • TS Over RTP
Type[2]	The type of distribution method: • Unicast • Multicast
Address/Port[1,2]	The port on which the server listens.
Network Interface	Identifies the network interface: • Auto • Eth0 • Eth1
SRT Settings[2] (Source)	
Mode	Specifies the SRT Connection Mode: • **Caller**: The SRT stream acts like a client and connects to a server listening and waiting for an incoming call. • **Listener**: The SRT stream acts like a server and listens and waits for clients to connect to it. • **Rendezvous**: Allows calling and listening at the same time. TIP: To simplify firewall traversal, *Rendezvous* mode allows the encoder and decoder to traverse some firewall configurations without the need for IT to open a port.

Route Setting	Description
Latency	Specifies the SRT receiver buffer that permits lost packet recovery. The size of this buffer adds up to the total latency. A minimum value must be 3 times the round-trip-time (RTT). Range = 20 - 8000 ms NOTE: Latency is for the SRT protocol only and does not include the capture, encoding, decoding and display processes of the end-point devices.
Passphrase	(Only required and accepted if Encryption is enabled on the Destination) Specifies a string used to generate the encryption keys to protect the stream. Range = 10-79 UTF8 characters
Destinations	
Name[1]	Name (limited to 60 printable characters). TIP: Keep the name under 18 characters to have the entire name displayed in the Browse Routes screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.
Protocol	Select from the drop-down menu one of the available streaming protocols: • TS Over UDP • TS Over SRT • TS Over RTP • HLS
Address / Port[1,2]	*For TS only:* Depending upon the type of SRT settings, this field may require an IP address of transmission and the listening port. NOTE: TS Over SRT only requires the Port field.
Segment Duration	*For HLS only:* Maximum media segment duration (in seconds). A target duration of 10 seconds is recommended, and is the default if no target duration is specified. Shorter segments may increase network overhead for the client. Longer segments will increase broadcast latency and initial startup time. NOTE: Apple strongly recommends a 10 second target duration. If you use a smaller target duration, you increase the likelihood of a stall. If you've got live content being delivered through a CDN, there will be propagation delays, and for this content to make it all the way out to the edge nodes on the CDN it will be variable. In addition, if the client is fetching the data over a cellular network there will be higher latencies. Both of these factors make it much more likely you'll encounter a stall if you use a small target duration.

Route Setting	Description
Encryption	*For HLS only:* Check this box to activate the default HLS encryption (AES-128 using 16-octet keys).
Segments/Key	*For HLS only:* If encryption is enabled, inserts a new random key file every **n** media segments (key rotation). Each group of **n** files is encrypted using a different key.
Link Parameters	
Port[1,2]	The port on which the server listens.
Network Interface	Identifies the network interface: • Auto • Eth0, Eth1 (may vary; options will include other available interfaces)
FEC[2]	(Only available on non-SRT streams) Enable Forward Error Correction (FEC). Select either: • (None) • VF (TS over UDP only) NOTE: VF FEC is a proprietary FEC and is not inter-operable with devices outside of the Haivision family.
Traffic Shaping[2]	(Only available on non-SRT streams) Check or clear this checkbox to enable or disable Traffic Shaping for the stream. For some limited networks such as satellites or some dedicated network pipes, it may be necessary to enable Traffic Shaping to smooth the traffic and respect the absolute upper limit configured. NOTE: Using Traffic Shaping on streams above 7Mbps may create audio/video artifacts (default configuration with medium to heavy movement video content).
Maximum Bitrate[2]	(Only available on non-SRT streams) Bitrate upper bound in kbps. Field is editable if the Traffic Shaping checkbox is selected.
MTU	(Maximum Transmission Unit) Specifies the maximum allowed size of IP packets for the outgoing data stream. 280..1500
TTL	(Time-to Live for stream packets) Specifies the number of router hops the Stream packet is allowed to travel/pass before it must be discarded. Value is higher or equal to 1.
ToS	(Type of Service) Specifies the desired quality of service (QoS). This value will be assigned to the Type of Service field of the IP Header for the outgoing streams.Value is higher or equal to 0.

Route Setting	Description
SRT Settings[2] (Destination)	
Type	The SRT connection (handshake) mode to be used with this destination: • Listener • Caller • Rendezvous
Latency	A fixed value (from 20 to 8000 ms) representing the maximum buffer size available for managing SRT packets. The minimum value on a fairly good network would be 3 times the round-trip-time (RTT). NOTE: Latency applies to the SRT protocol only and does not include the capture, encoding, decoding and display processes of the end-point devices.
Bandwidth Overhead	The percentage of the average bandwidth* that is used to accommodate SRT controls as well as recovery of lost packets. Range = 5-100% (default value is 25%) NOTE: SRT streams may temporarily overshoot the defined bandwidth overhead limit. * The "average bandwidth" is an internal measurement of the outbound traffic, on a per stream basis.
Encryption	The encryption, if any, to be applied to the SRT stream: None, AES-128, or AES-256.

1. Required field.
2. Field availability depends upon other selections made.

7. When you have finished entering the required data, click the Create button to specify the destination. Note: The newly created destination is added locally (at this point, no server call is made).
8. When finished entering all your destinations, click Apply. Now the configurations, including route, source, and destination(s), are saved to the server.

   The route listings should now be updated appropriately. Use the Expand All *button to view Source and Destination specifics.*

Related Topics

- "Editing a Route" on page 52
- "Starting/Stopping/Deleting a Route" on page 52
- "Viewing a Route's Statistics" on page 53
- "Adding a Route's Destination" on page 58

Editing a Route

To edit a route:

1. On the BROWSE ROUTES screen, click the Route Name for the listing you want to edit.
2. In the the EDIT ROUTE screen, adjust the settings as desired.
3. Click the Apply button to save the new settings.

Related Topics

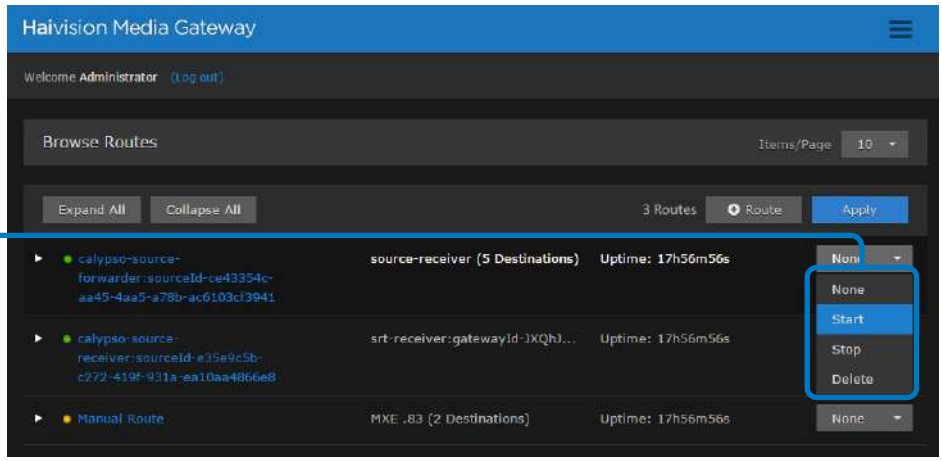
- "Creating a Route" on page 45
- "Available Route Settings" on page 48
- "Adding a Route's Destination" on page 58
- "Starting/Stopping/Deleting a Route" on page 52
- "Working with Routes" on page 45
- "Viewing a Route's Statistics" on page 53

Starting/Stopping/Deleting a Route

NOTE
Starting a route also starts its source and destination(s).

To start a route:

1. On the BROWSE ROUTES screen, locate the desired route listing and select Start, Stop, or Delete from the drop-down menu at the end of the listing.



2. Click Apply.

Related Topics

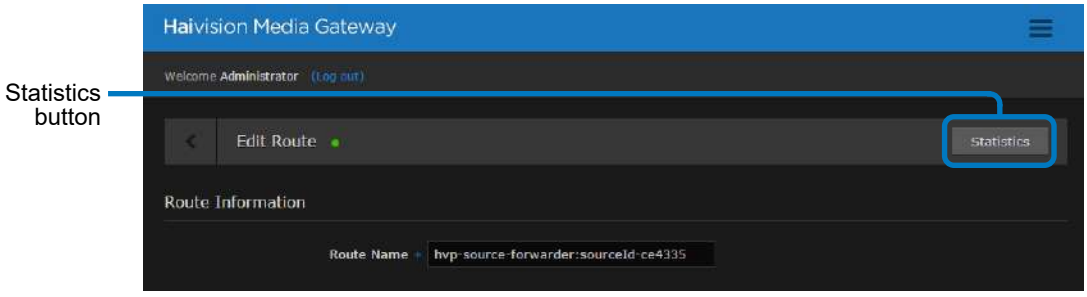
- "Creating a Route" on page 45
- "Available Route Settings" on page 48
- "Adding a Route's Destination" on page 58
- "Editing a Route" on page 52
- "Viewing a Route's Statistics" on page 53

Viewing a Route's Statistics

A route's statistics gives you access to real-time data regarding the route's source and destinations.

To view statistics for a route:

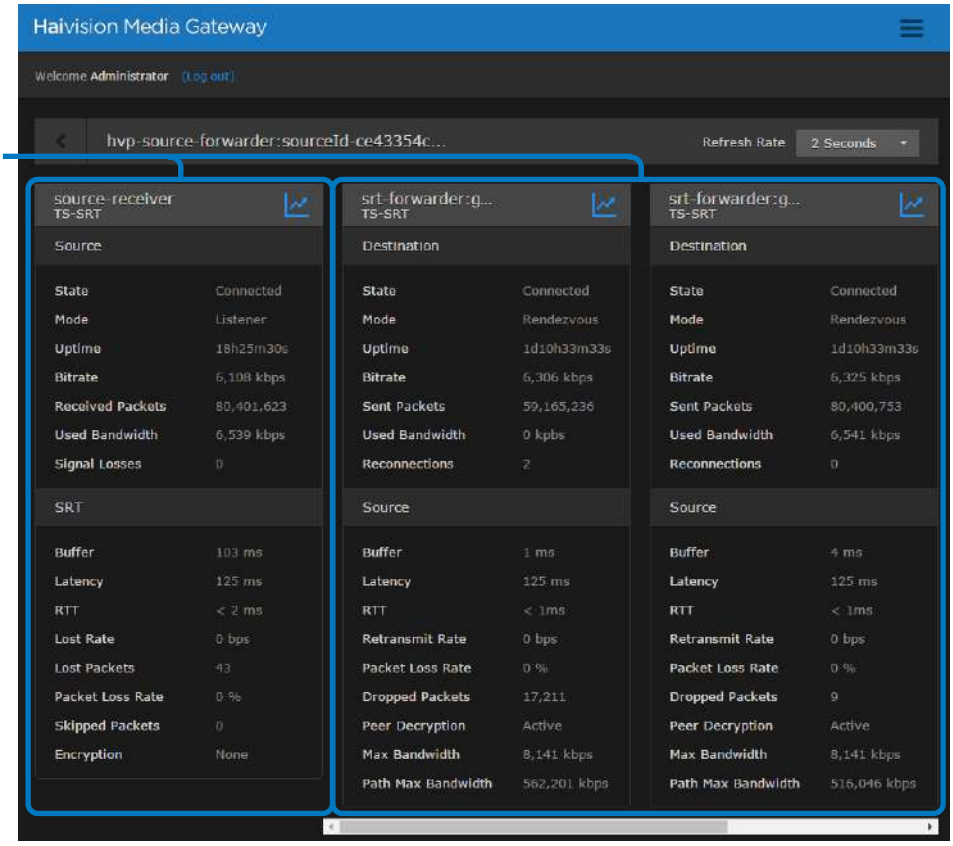
1. On the BROWSE ROUTES screen, click on the the desired route listing to open the Edit Route page.
2. Click the Statistics button in the title bar.



3. When the Statistics Overview page appears, you can view the pertinent data for the routes' source and destinations.

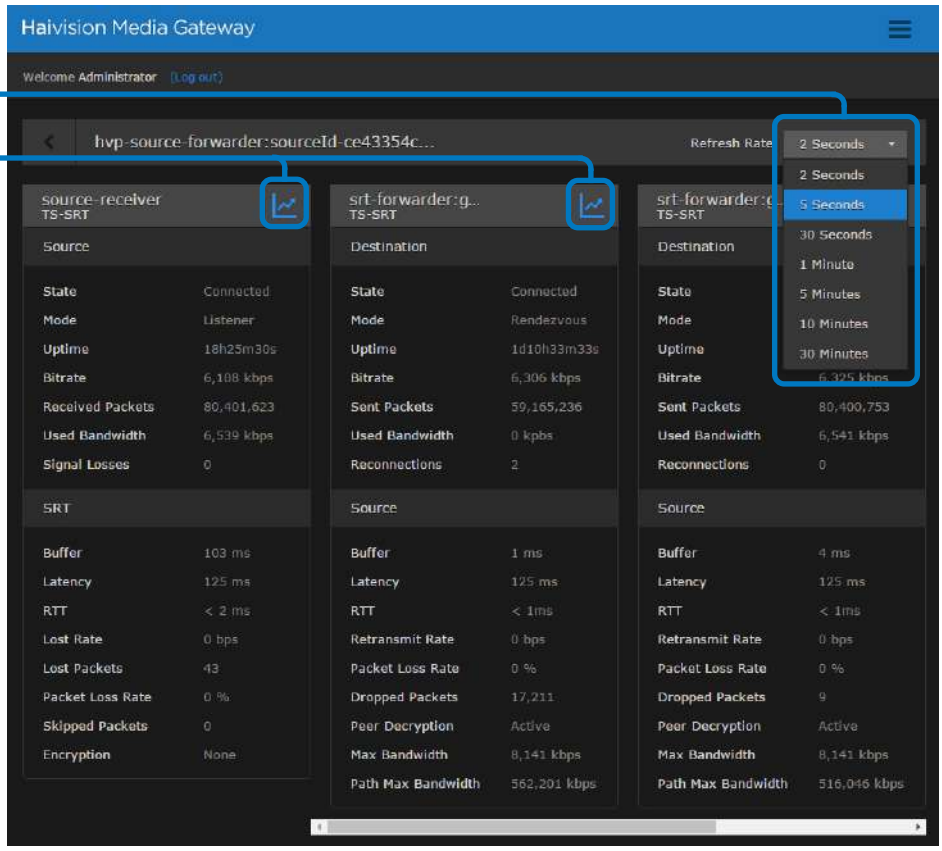
The information for the source and destination(s) appears in a column identified by the name and protocol in the heading.

The column sections are organized by Type.



Typically, the Statistics fields order of appearance is consistent. However, a field is not displayed if it has no value.

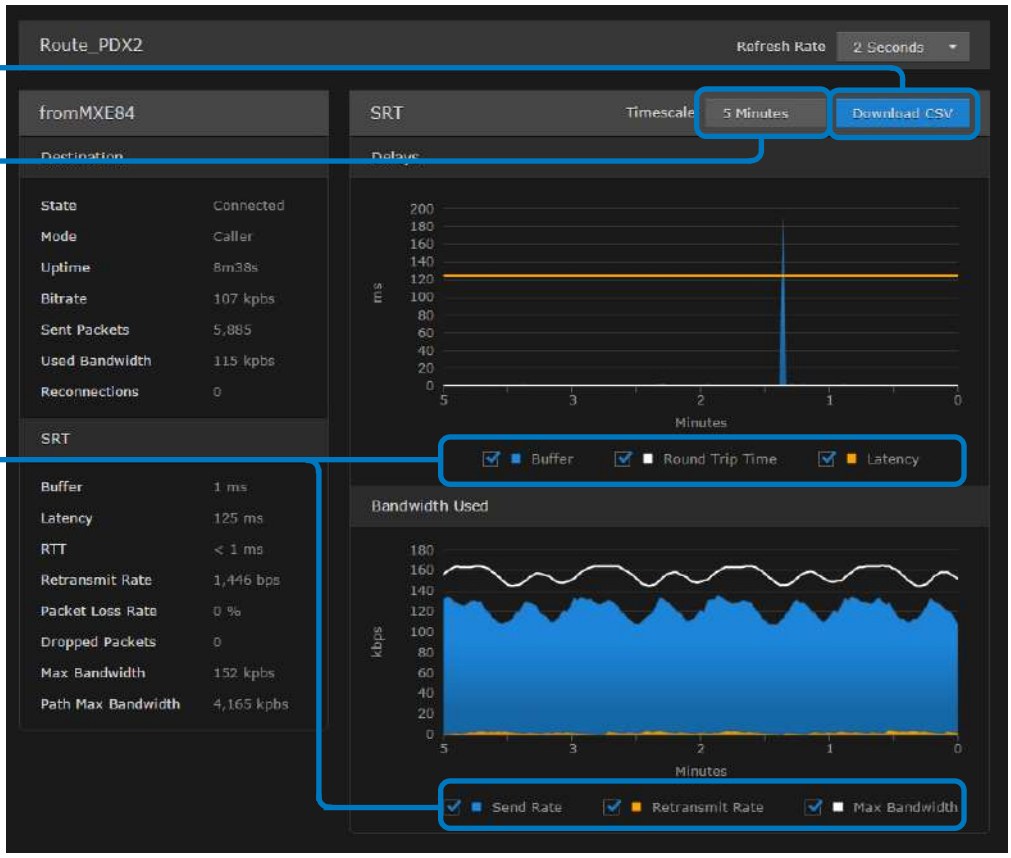
4. To change the refresh rate, click the associated drop-down menu.



5. To view the data graphically, click the  icon for the desired route.

When the Statistics Graph View window opens, it displays the data numerically and graphically for that route. This window opens separately so that you can keep it open

for monitoring — even create a dashboard of one or more devices. This window remains open until you manually close it.



6. To save the data for use with another application (such as a spreadsheet), click the Download CSV button. Typically, this downloads the data in a comma-separated values text file. For Safari browsers, this displays the file in a new window. Right-click the browser window and select "Save Page as..." to download the file.

7. You can adjust the real-time graph by:
   - Setting the Refresh Rate with the drop-down menu in the title bar.
   - Changing the scale interval using Timescale drop-down menu. This adjusts the x-axis in the graphs. Options include: 5 minutes, 1 hour, and 24 hours.
   - Checking/unchecking the checkboxes of each legend to display/hide data components.

- Hover your mouse cursor over the graph to reveal the time and value of the selected data point.

Related Topics

- "Creating a Route" on page 45
- "Available Route Settings" on page 48
- "Adding a Route's Destination" on page 58
- "Starting/Stopping/Deleting a Route" on page 52
- "Reports (Logs)" on page 67

Working with Destinations

NOTE

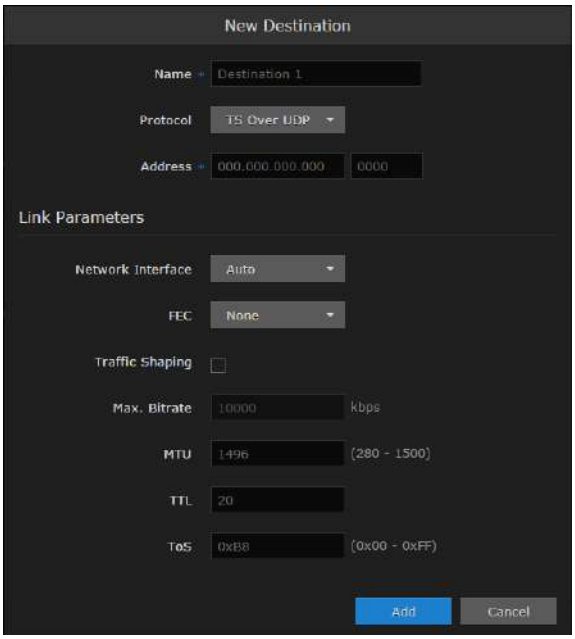
Keep in mind that **route actions**, when applied, override all the Destination states. For instance, performing a stop action on a route, once applied, stops any destinations for the route as well.

Adding a Route's Destination

Destinations are not started automatically.

To add a destination:

1. On the BROWSE ROUTES screen, click on a route that you want to add a destination to.
2. On the Edit Route page, click the +Destination button.
3. In the New Destination dialog, provide appropriate settings for the Destination. See "Destinations" on page 49 for field specifics.



4. When finished, click the Add button.
5. If you want to start the destination, use the Destination's action menu and select Start.

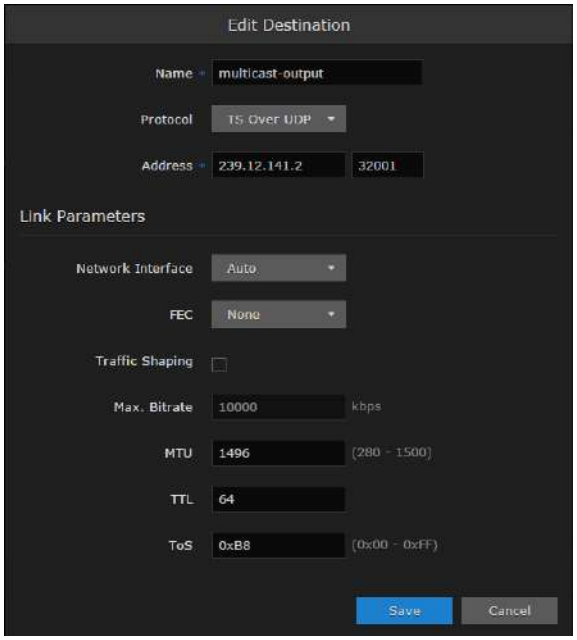
6. When finished adding destinations, click Apply.

IMPORTANT
Destination operations (Add, Edit and Actions), are not saved to the server until the Apply button is clicked on the EDIT ROUTE page.

Editing the Destination

To change the Destination settings:

1. On the BROWSE ROUTES screen, click the individual ▶ icon or the Expand All button to reveal the destination specifics for the route.
2. Locate the destination you want to configure and click it to open the Edit Destination dialog.
3. On the EDIT DESTINATION dialog, adjust the settings as desired. See "Destinations" on page 49 for definitions of the fields.



4. Click the Save button.

The new settings appear in the Destination section for the route.

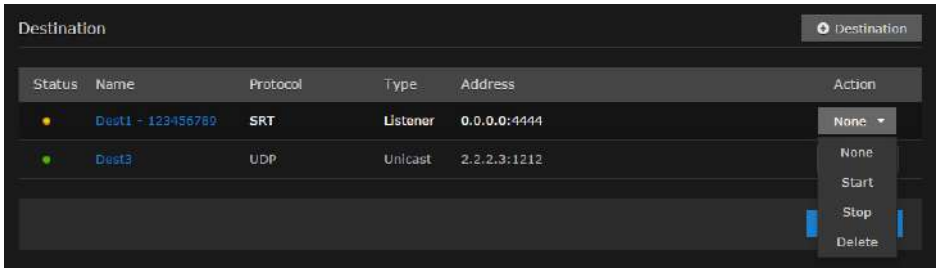
IMPORTANT

Destination operations (Add, Edit and Actions), are not saved to the server until the Apply button is clicked on the BROWSE ROUTES screen.

Starting/Stopping/Deleting a Destination Node

To start, stop, or delete a destination node:

1. On the BROWSE ROUTES screen, click on the desired route to open the Edit Route page.
2. On the Edit Route page, locate the desired destination listing.
3. Click the drop-down menu at the end of the listing and select the Start, Stop, or Delete option. If there are other destinations that you want to stop, start, or delete, do so now.



4. Click Apply for your requested action(s) to take effect.

NOTE

If the route is stopped, the Start/Stop options are not available.

CHAPTER 4: Performing Admin Tasks

The following content explains how to manage Media Gateway settings and status, including system activity, network settings, and security.

NOTE

The intended audience for this content is system integrators and administrators with administrative privileges.
For information on options and tasks available to non-administrative users, such as browsing routes, please refer to "Working with Media Gateway" on page 28.

Topics Discussed

System Activity

Media Gateway includes dashboards as a management tool to provide a quick view of the overall system health:

- System Activity
- Reports (Logs)

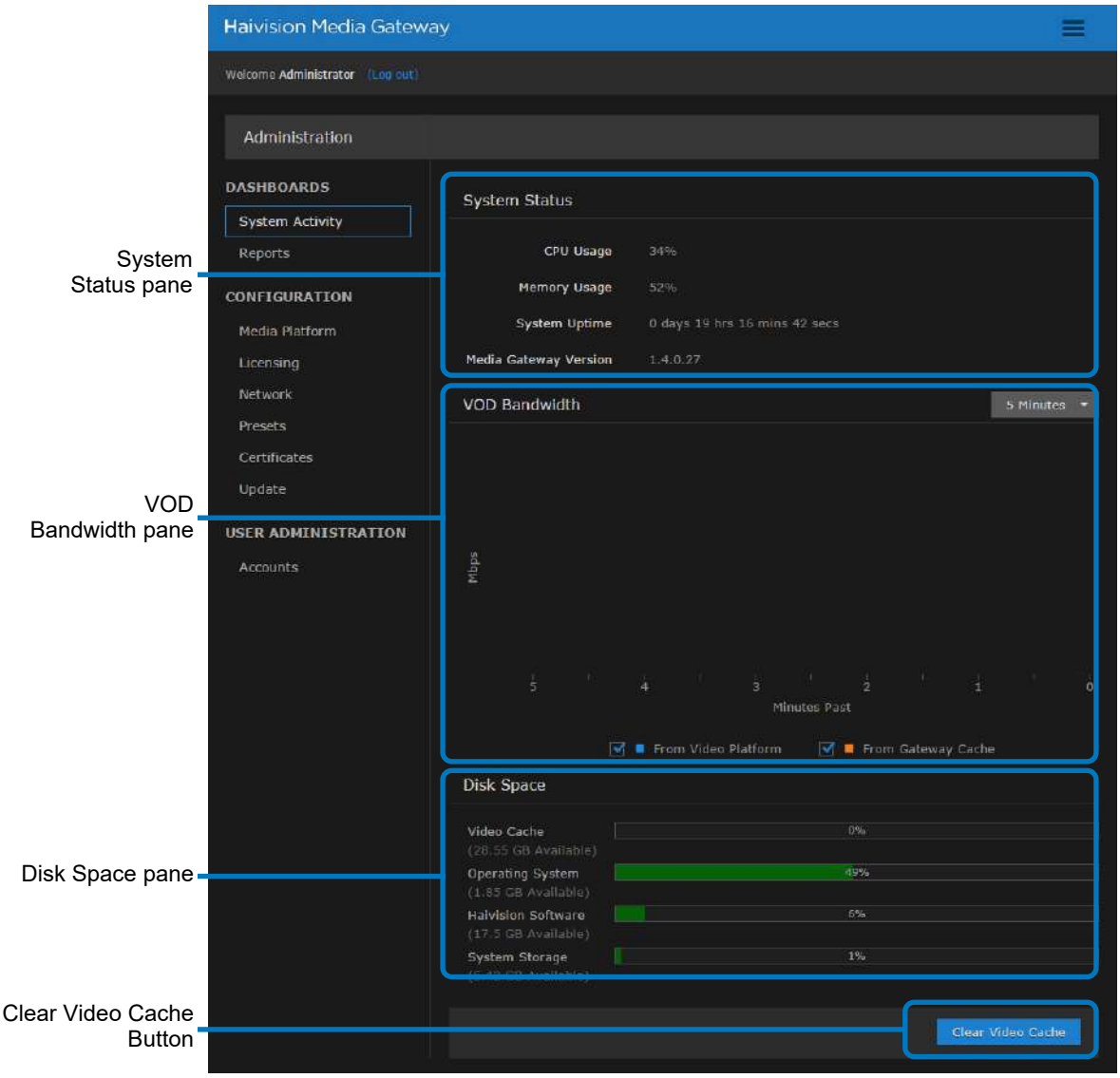
Viewing the System Activity Dashboard

The System Activity dashboard shows the current status snapshot of your system as a whole, including disk space and Media Platform bandwidth.

To view the system's activity dashboard:

1. Click the  icon on the toolbar and click **Administration**.
2. Click System Activity in the sidebar.

The System Activity dashboard appears.



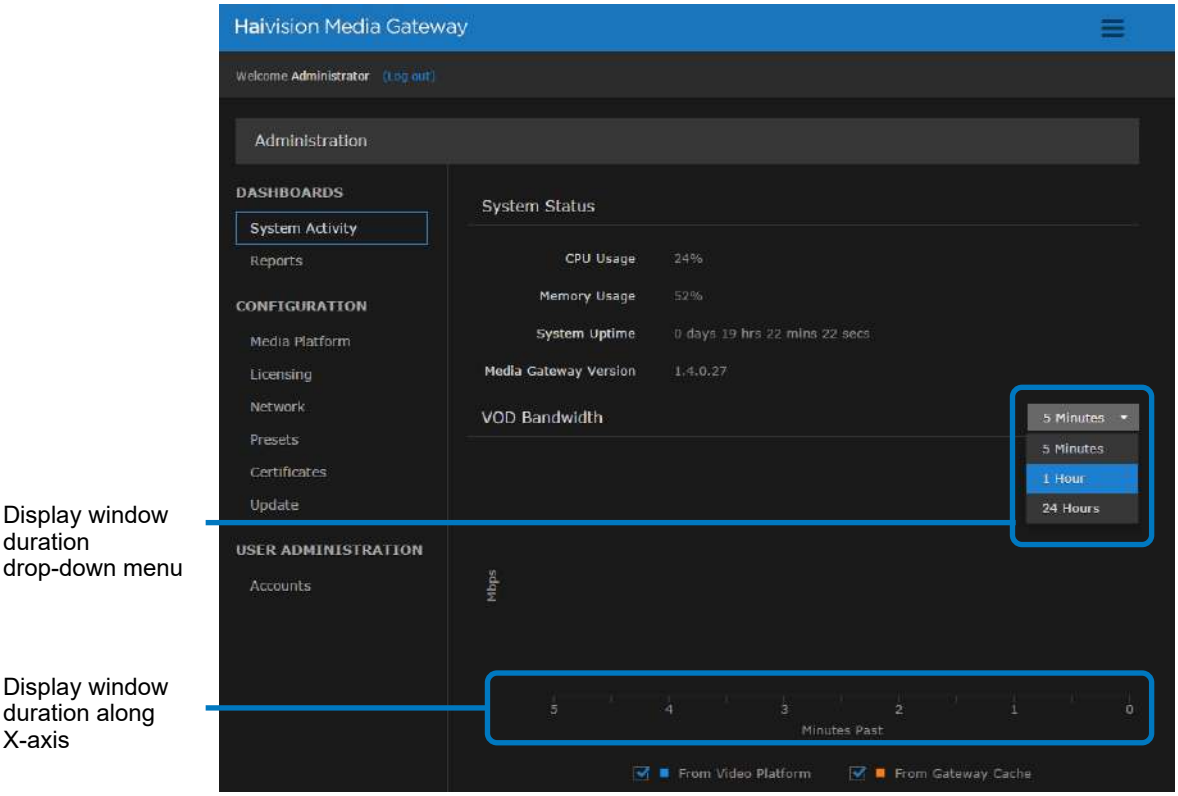
The *System Status* pane provides the following information:

- CPU usage
- Memory usage
- System uptime
- Media Gateway version

The *VOD Bandwidth* pane charts usage in Mbps. The checkboxes below the graph allow you to tailor the display to include information from Media Platform, the cache, or both.

Use the drop-down menu at the top of the chart to specify the *display window* for the graph starting from now (that is, "0"). When the actual timeframe exceeds the specified display window, only the most recent data of the specified length of time is displayed.

That is, if 5 Minutes is selected, only the last five minutes of data is displayed. Any data older than five minutes is dropped from the graph.



In the *Disk Space* pane, you see information regarding disk usage.

Disk Space	Corresponding Directory/Partition Location
Video Cache	/assets
Operating System	/
Haivision Software	/opt
System Storage	/var

The bars are color-coded to alert you as designated space reaches usage thresholds:

Bar Color	Indicates Usage Threshold
	0–74% of the space is in use. *Only 25% remains available.*
	75–90% of the space is in use. *Only 10% remains available.*
	90–100% of the space is in use.

Click Clear Video Cache to delete all of the locally-cached video previously downloaded from Media Platform. When prompted to confirm, click Clear.

Related Topics

- "Viewing a Route's Statistics" on page 53
- "Reports (Logs)" on page 67
- "Clearing the Video Cache" on page 66
- "Viewing the Status of a License" on page 76
- "Downloading System Updates" on page 93
- "Viewing the Media Gateway Version Number" on page 76

Clearing the Video Cache

When streaming, it may be necessary to clear the cached videos.

To clear the video cache:

1. Click the  icon on the toolbar and click **Administration**.
1. Click System Activity in the sidebar.
2. In the *Disk Space* pane, click the Clear Video Cache button to delete all the locally-cached video previously downloaded from Media Platform.
3. When prompted to confirm, click Clear.

Related Topics

- "Viewing a Route's Statistics" on page 53

Reports (Logs)

Media Gateway generates a number of different logs providing system, application, and diagnostic messages. These logs are described in the following table:

Log Name	Description
All Logs	All system and application logs. Includes the Media Gateway logs and System messages.
System Messages	Operating system messages. Includes /var/log/messages.
Media Gateway	Log data from the Media Gateway processes. Including: • madra_log_query — logs from the past week. • /opt/haivision/var/log/kulabyte — KB Encoder logs, if present.

Enabling Diagnostic Logging

From the REPORTS screen, you can switch on and off diagnostic logging. By default, logging is disabled.

To enable logging:

1. On the ADMINISTRATION screen, click Reports on the sidebar.
2. Toggle the Enable Diagnostic Logging button to On.
3. Click Save Settings.

IMPORTANT

Diagnostic logging impacts system performance and should be enabled *only* as a temporary troubleshooting measure. Diagnostic files are not deleted automatically and eventually consumes all available disk space if left enabled.

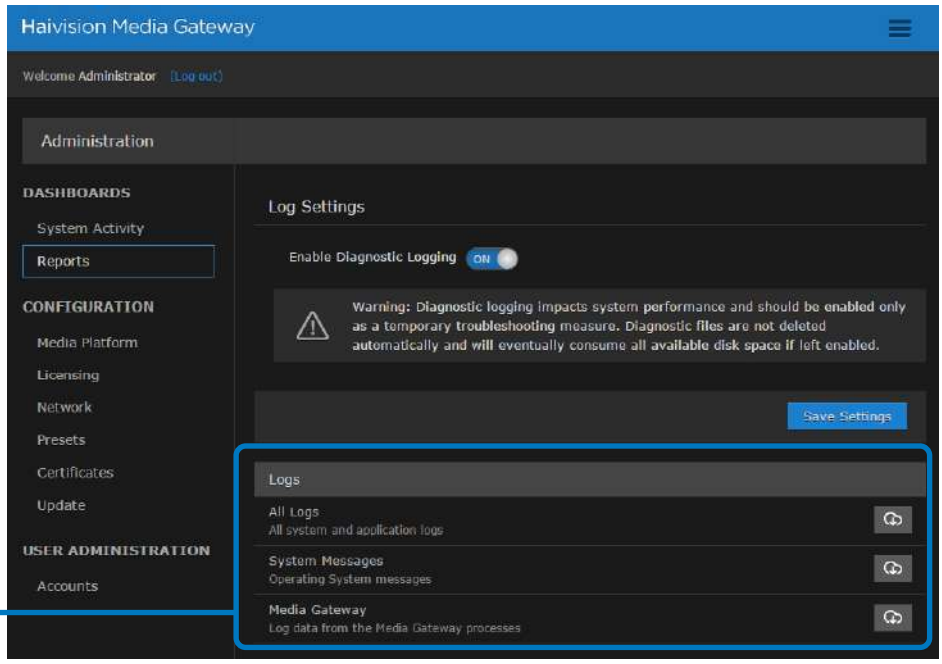
Viewing Reports (Logs)

From the REPORTS screen, you can also download reports and logs.

To view a log:

1. On the ADMINISTRATION screen, click Reports on the sidebar.

The view pane consists of the Logs pane.



2. In the Logs pane, click the desired log's icon to download a zip file of the log's text files.
3. If you select "All Logs," open the zip file and browse the folder structure:

   `Media_Gateway > opt > haivision > var > log`

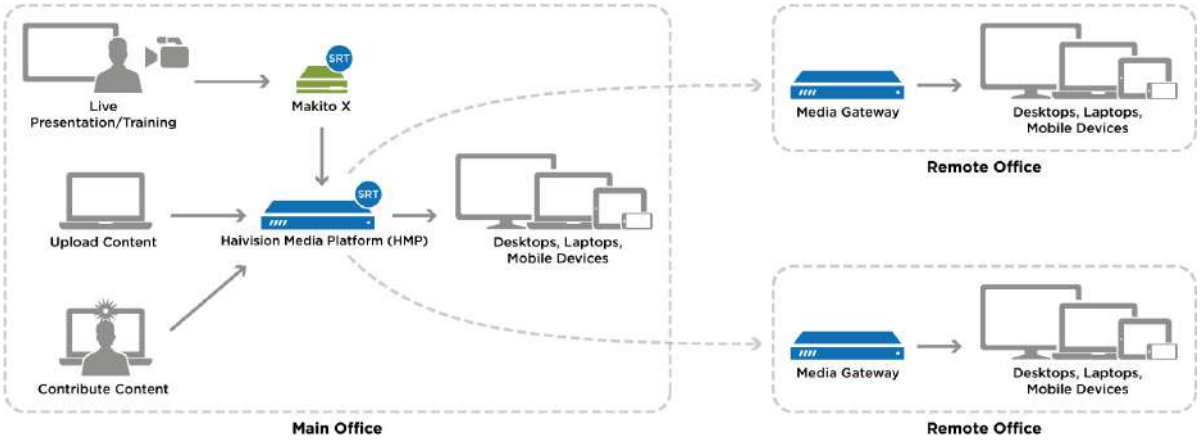
   The log *folder is populated with text log files with descriptive filenames to assist you in identifying the appropriate file for the information you seek.*

Related Topics

- "Viewing a Route's Statistics" on page 53
- "Viewing the Status of a License" on page 76
- "Downloading System Updates" on page 93
- "Viewing the Media Gateway Version Number" on page 76

Media Platform

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



Media Gateway integration with Media Platform

Pairing Media Gateway with a Media Platform Server

Media Gateway devices initiate outbound requests to Media Platform to avoid issues with firewall transversal. As a security measure, the Media Platform Pairing Passcode is "Disabled" by default to block any pairing requests. Pairings may be deleted from Media Platform, but are otherwise managed from the Media Gateway web interface. The following procedures step you through the tasks needed to be performed:

- "Creating your Ecosystem Workspace" on page 69
- "Acquiring a Pairing Passcode" on page 70
- "Pairing the Devices" on page 71

Refer to your Media Platform documentation for information on using Media Gateways and how to set up locations for routing users to the closest Media Gateway for the best streaming experience.

Creating your Ecosystem Workspace

Use browser tabs to switch easily between the Media Platform server and Media Gateway interfaces.

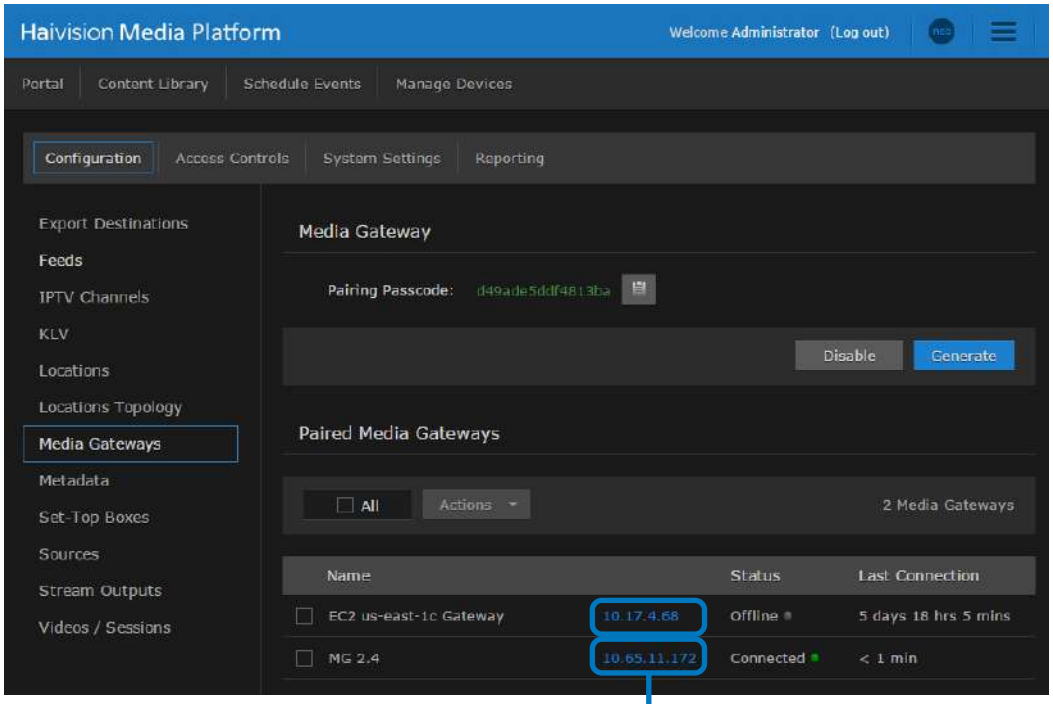
To create your workspace:

1. In your browser, open a tab and enter the URL for the Media Platform server.

2. Open another browser tab and enter the URL to the Media Gateway.

TIP

Within the Media Platform ADMINISTRATION screen's Media Gateways panel, you can use the action links (blue) in the Paired Media Gateway listing to open a tab to a particular Media Gateway web interface.



Action links open a tab to their corresponding Media Gateway.

Acquiring a Pairing Passcode

To initiate pairing between the Media Gateway with Media Platform, you must acquire a *pairing passcode* from the Media Platform server. The passcode is only needed for the initial pairing and not on an ongoing basis.

To acquire the passcode:

1. In your Media Platform browser tab, click the icon and click Administration.
2. Click Media Gateways in the sidebar.
3. If the Pairing Passcode field is empty or disabled, click Generate to create a new pairing passcode.
4. Copy the pairing passcode to the clipboard.

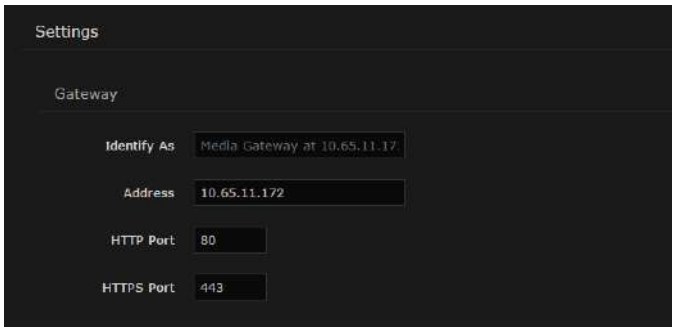
5. Make note of the Media Platform address and ports. If there is a cross-domain address, make a note of it as well.

Pairing the Devices

To pair the devices, you need to supply the addresses and ports that are being used, as well as the Media Platform pairing passcode. If you haven't already acquired this information, refer to the previous section, "Acquiring a Pairing Passcode".

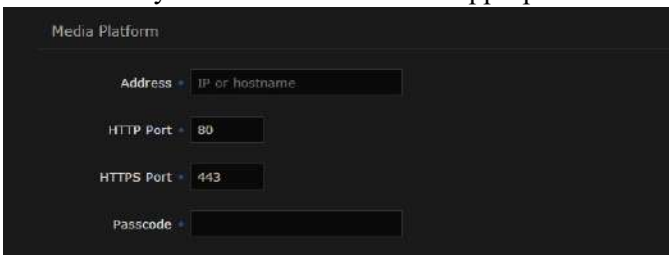
To pair the devices:

1. In your browser tab of the Media Gateway you wish to pair with the Media Platform, click the  icon and click Administration.
2. Click Media Platform in the sidebar.
3. In the Gateway section of the Settings pane, enter the Media Gateway information as needed:



   - **Identify As**— a descriptive or more user-friendly name for indicating the Media Gateway.
   - **Address** — the URL for the Media Gateway.
   - **HTTP Port**
   - **HTTPS Port**

4. In the Media Platform section of the Settings pane, enter the Media Platform information that you noted earlier into the appropriate data fields:

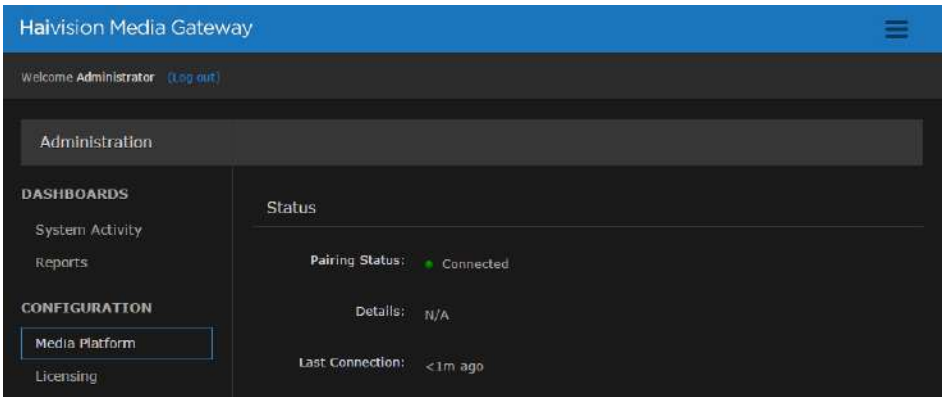


   - **Address** — the URL that the Media Gateway uses to connect with the Media Platform server; that is, the private (inside the firewall or VPN) IP/hostname for the Media Platform.

- **Cross-Domain Address** — the address used to host the Media Platform to the end users; that is, the public-facing IP/hostname for the Media Platform. Typically only necessary when deploying.
- **HTTP Port**
- **HTTPS Port**
- **Passcode** — Paste the passcode from your clipboard into the Passcode field.

5. Click Pair.

   When the connection is made, the status indicator in Pairing Status turns green.



TIP

While the pairing is in progress, you can switch to the browser's Media Platform tab to see the status indicator turn green when the connection is made.

If the **Pairing Status** on the (Media Gateway) MEDIA PLATFORM screen displays the message "Pairing timeout", this may be an indication the Media Platform server is unavailable. Try the following:

- Check your local network.
- Confirm the availability of the Media Platform with which you are attempting to pair.
- Click the Clear button and enter settings for an alternate Media Platform.

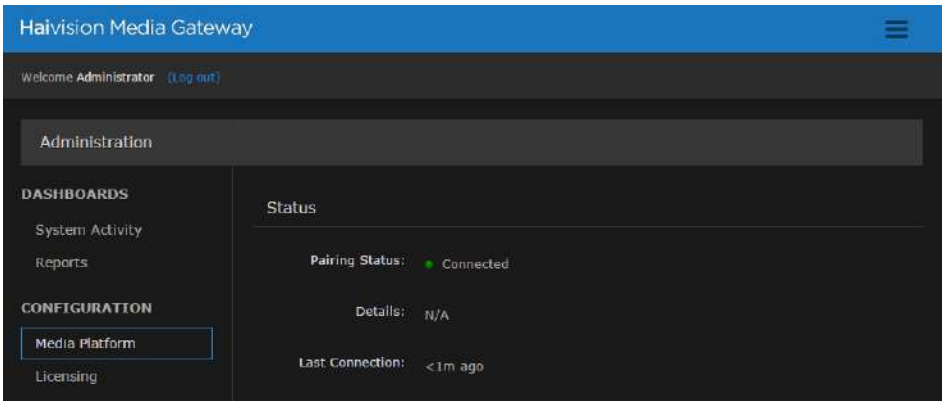
Viewing the Status of Media Gateway Connections

To determine the status of a Media Gateway connection:

1. On the (Media Gateway) MEDIA PLATFORM screen, hover your cursor over the status icon or use the following color codes:
   - Green — Connected (Poll requested succeeded within the last 5 minutes).
   - Yellow — Warning (Pairing is pending, or some potentially transient error).

- Red — Error (Last poll request failed due to authorization, 404, or pairing timeout).
- Gray — Disconnected (Last poll response was received over 5 minutes ago).

2. The MEDIA PLATFORM screen also tracks the connection's duration in the Last Connection field.



Blocking New Media Gateway Connections

To block any new Media Gateway connections:

1. In your Media Platform browser tab, click the icon and click Administration.
2. Click Media Gateways in the sidebar.
3. Click the Disable button under Pairing Passcode.

Updating the Media Platform Server

To update the Media Platform server:

1. In your Media Gateway browser tab, click the icon and click Administration.
2. Click Media Platform in the sidebar.
3. Change one of the settings, such as update the "Identify As" name to something new.
4. Click Update so that the new information is updated on the Media Platform server.

Clearing the Media Platform Server

When there is a pairing error, the Disconnect button becomes a Clear button to allow you to clear the error record and the pairing status returns to “Not paired”.

To clear the Media Platform server:

1. In your Media Gateway browser tab, click the  icon and click Administration.
2. Click Media Platform in the sidebar.
3. Click the Clear button.
4. Click Confirm to verify that you want to clear the cache of the entries.

Disconnecting from a Media Platform Server

To disconnect from a Media Platform server:

1. In your Media Gateway browser tab, click the  icon and click Administration.
2. Click Media Platform in the sidebar.
3. Click the Disconnect button.
4. Click Confirm to verify that you want to disconnect from Media Platform.

Licensing

This section provides instructions to update your Media Gateway license. Any update other than a maintenance release (for example, v1.1.*x*), requires a new license.

IMPORTANT

Please contact Haivision Technical Support to obtain a valid license key if needed. Without a valid license key, you can log in. However, you won't be able to create or edit routes until you have imported a license.

Adding a license to the Media Gateway server requires administrator privileges and a license key.

When a system is not licensed, the BROWSE ROUTES page displays a LICENSE REQUIRED warning dialog. If the user's role is administrator, the dialog displays an Add License button.

Adding a Media Gateway License

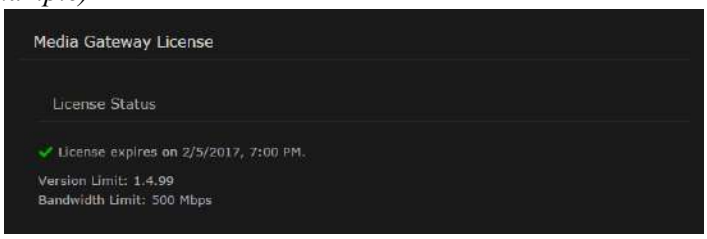
To license Media Gateway:

1. After logging into the web interface, if you see a LICENSE REQUIRED dialog, click Add License.

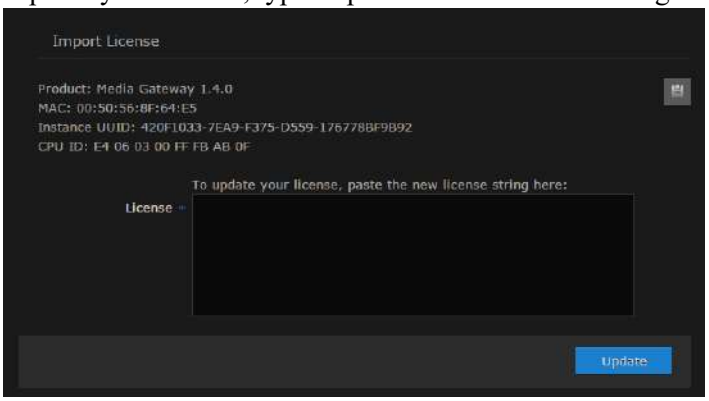
   -or-

   Click the  icon, click Administration, and click Licensing in the sidebar.

   The Licensing view pane shows status information for the installed Media Gateway license, including its expiration date, version limit, and bandwidth limit (see following example)



2. To update your license, type or paste the new license string in the text box.



3. Click Update to load the license.

   The License Status is updated to show the new license information.

TIP

To copy the current license details to the clipboard, click .

Related Topics

- "Viewing the Status of a License" on page 76

Viewing the Status of a License

License information includes the expiration date, version limit, and bandwidth limit.

To view the status of a Media Gateway license:

1. Click the icon and click Administration.
2. Click Licensing in the sidebar menu.

The license status information is shown in the Licensing view pane.

Related Topics

- "Adding a Media Gateway License" on page 75

Viewing the Media Gateway Version Number

Option 1:

1. Click the icon and click About Media Gateway.

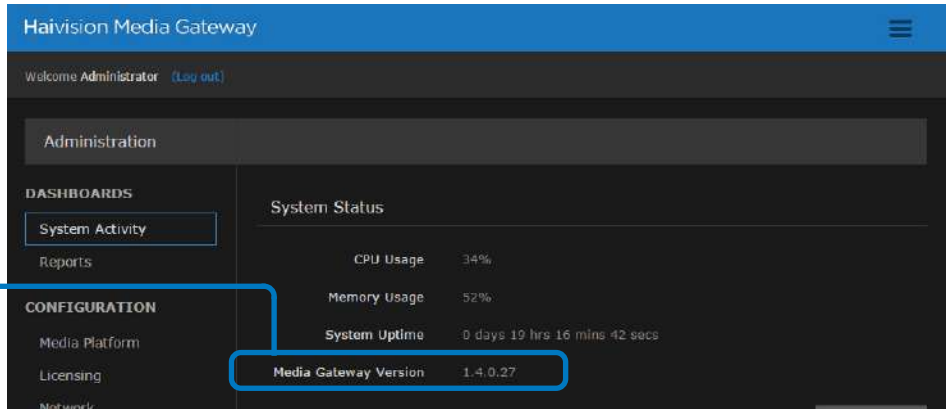
The About Media Gateway dialog opens to display the version information for the current installation.

2. When finished, click Close to exit the dialog.

Option 2:

1. Click the icon and click ADMINISTRATION.
2. Click System Activity in the sidebar menu.

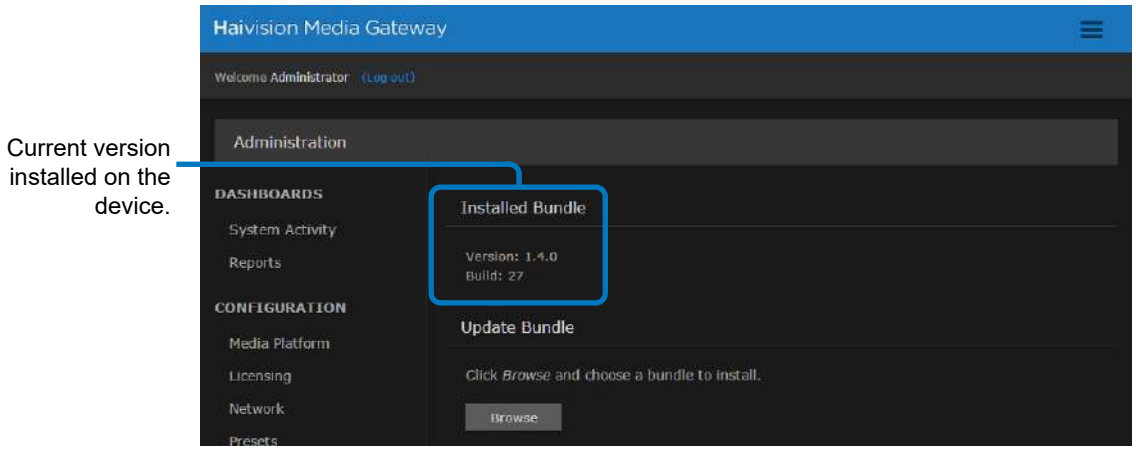
   The Media Gateway version is listed under System Status.



Option 3:

1. Click the icon and click ADMINISTRATION.
2. Click Update in the sidebar menu.

The Media Gateway version is listed under Installed Bundle.



Related Topics

- "Downloading System Updates" on page 93
- "Installing/Updating a Package (HaiBundle)" on page 93

Network

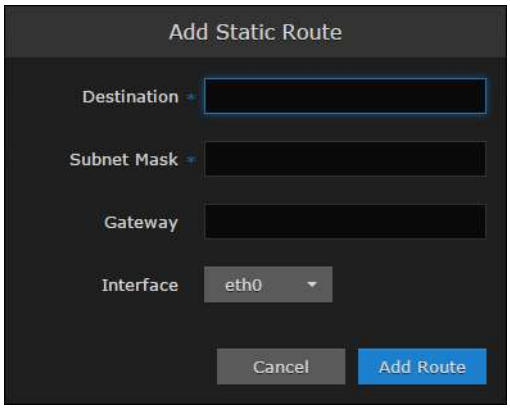
The Network Configuration settings allow you to specify the server hostname, DNS servers, NTP server, search domains, and the default interface. This is also the screen where you configure advanced settings for multiple network interfaces, NIC bonding, and static routes.

Configuring the Network

To configure the network:

1. Click the icon and click ADMINISTRATION.
2. Click Network in the sidebar menu.

   The available network configuration settings are listed in the view pane along with Interfaces and Static Routes.
3. Fill in the fields as appropriate. See "Network Settings" on page 80 for more information.
4. To configure multiple network interfaces, after you complete eth0, select the next interface (e.g., eth1) and repeat the configuration.
5. To add a bond interface, see "Creating a Bonded Interface" on page 83 for more information.
6. To add a Static Route, click +Route and provide the necessary data in the Add Static Route dialog.



7. Click Add Route. The Static Route is added to the listings on the Network Configuration screen.
8. Click the Save Settings button.
9. Click the Reboot button to have your network configuration changes take effect.

Network Settings

Table 1. Network Settings

Network Setting	Description
General	
Hostname	The hostname to be assigned to the Media Gateway. Specify the hostname as a fully-qualified domain name (FQDN). For example: myserver.mycompany.com
Default Interface	The default Ethernet interface is eth0.
DNS Servers	*(Optional)*. The Internet Protocol version 4 (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 the Network Time Protocol (NTP) is enabled, enter the IP address of the NTP server.
SNMP	Enable/Disable Simple Network Management Protocol (SNMP).
Read-Only Community	SNMP string to be used when making read-only information requests.
SNMP Trap Servers	IPv4 or FQDN of a server to send SNMP traps to.
Interfaces	
eth0 | eth1 | eth2 | ...	Allows for multiple interfaces. Select the appropriate tab to view and configure.
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.
Addressing	Choose whether the interface uses a static or dynamic IP address: • None — Select to disable the interface. • Static — Select to disable DHCP. When it is disabled, you must manually enter the IP address and subnet mask. • DHCP — Select to enable the Dynamic Host Configuration Protocol. When DNCP is enabled, the appliance will receive an IP address from a DHCP server on the network.

Table 1. Network Settings (Cont.)

Network Setting	Description
IP Address	Displays the IP Address. This is a unique address that identifies the unit in the IP network. NOTE: If DHCP is disabled, you may enter an IP address in dotted-decimal format.
Subnet Mask	This is a 32-bit subnet mask used to divide an IP address into subnets and specify the network's available hosts. NOTE: If DHCP is disabled, you may enter the Network Mask in dotted-decimal format (e.g., 255.255.0.0).
Gateway	The IPv4 default route to be assigned to the interface. This is the gateway that is used when no other route matches. This address must be reachable on your local subnet. NOTE: If DHCP is disabled, you may enter the 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).
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. • Round Robin Sequential: Transmits packets in first available network interface (NIC) slave through the last. This mode provides load balancing and fault tolerance. • Active Backup: Only one NIC slave in the bond is active at a time. A different slave becomes active only when the active slave fails. This mode provides fault tolerance. • XOR Sequential: Transmits based on XOR formula. (Source MAC address is XOR'd with destination MAC address). This mode selects the same NIC slave for each destination MAC address and provides load balancing and fault tolerance.

Table 1. Network Settings (Cont.)

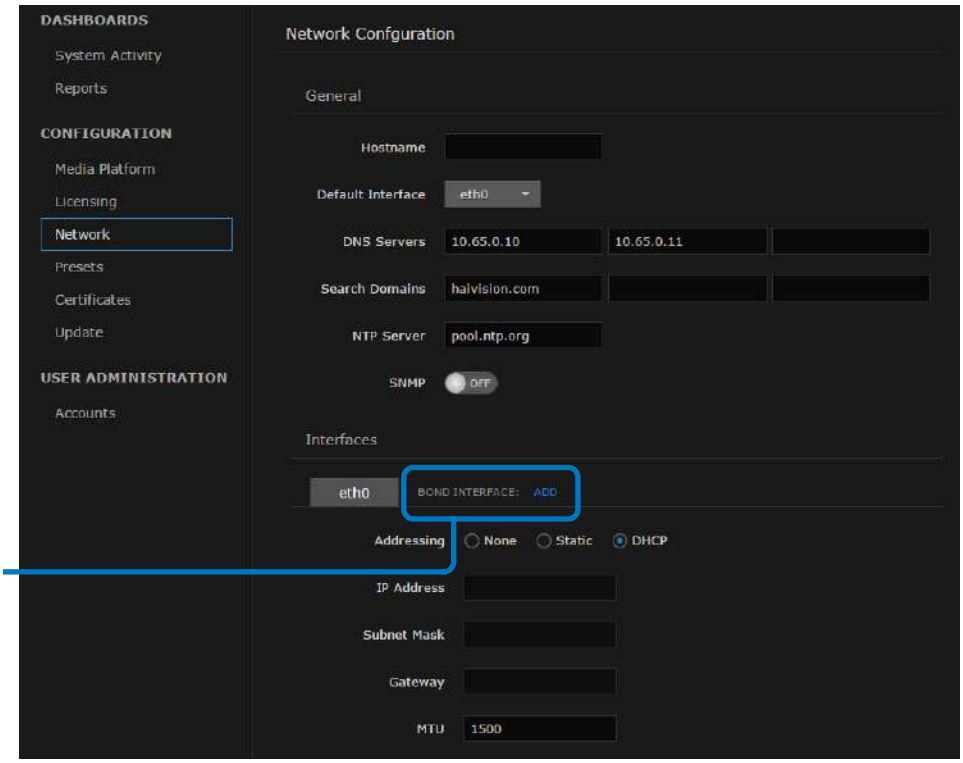
Network Setting	Description
Bonding Mode (Cont.)	• Broadcast – Fault Tolerance: Transmits network packets on all slave interfaces. This mode is least used (only for specific purpose) and provides only fault tolerance. • IEEE 802.3ad Dynamic Link Aggregation: Creates aggregation groups that share the same speed and duplex settings. Utilizes all slave network interfaces in the active aggregator group according to the 802.3ad specification. This mode is similar to the XOR mode above and supports the same balancing policies. The link is set up dynamically between two LACP-supporting peers. • (Adaptive) Transmit Load Balancing (TLB): The outgoing traffic is distributed according to the current load and queue on each slave interface. Incoming traffic is received by one currently designated slave network interface. If this receiving slave fails, another slave takes over the MAC address of the failed receiving slave. • (Adaptive) Active Load Balancing (ALB): This includes balance-tlb + *receive load balancing* (rlb) for IPV4 traffic. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the server on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different clients use different hardware addresses for the server.
Slave Interfaces	(Bond Interface only) Check this checkbox to enslave the primary interface (e.g., eth0) to the bond interface (e.g., BOND0).
Static Routes	
Destination	Each static route requires a destination.
Subnet Mask	This is a 32-bit subnet mask used to divide an IP address into subnets and specify the network's available hosts. NOTE: If DHCP is disabled, you may enter the Network Mask in dotted-decimal format (e.g., 255.255.0.0).
Gateway	This is the gateway that is used when no other gateway matches. This address must be reachable on your local subnet. If DHCP is disabled, you may enter the gateway address in dotted-decimal format.
Interface	The interface associated with the static route.Use the drop-down menu to make your selection.

Creating a Bonded Interface

Interface bonding provides a method for aggregating multiple network interfaces into a single logical interface. The goal is to increase throughput and to ensure redundancy in case one of the links fails.

To create a bonded interface:

1. Click the icon and click ADMINISTRATION.
2. Click Network in the sidebar menu.
3. Verify that the correct interface (for example, eth0) is currently selected.
4. Click the Bond Interface: Add action link.



The Bond0 tab appears and the Bond Interface: Remove action link replaces the Add action link.

5. Clink the Bond0 tab to reveal the bonding-specific fields (such as Bonding Mode and Slave Interface). See "Network Settings" on page 80 for more information.
6. Click the Save Settings button.
7. Click Reboot to have your changes take effect.

Removing a Bonded Interface

To remove a bonded interface:

1. Click the  icon and click ADMINISTRATION.
2. Click Network in the sidebar menu.
3. Verify that the correct bonded interface you wish to remove (for example, bond0) is currently selected.
4. Click the Bond Interface: Remove action link.

   The selected interface tab is removed.
5. Click the Save Settings button.
6. Click Reboot to have your changes take effect.

Presets

The System Presets screen allows you to export the current configuration as a preset file with .hmg extension. It also allows you to import an exported preset file and apply the preset to the device.

Exporting and Importing Presets

To export a preset:

1. Click the  icon and click ADMINISTRATION.
2. Click Presets in the sidebar menu.
3. To export a preset of the current system (device) route's configuration, click Export Preset.

   The browser downloads a .hmg file.

To import a preset:

1. Click Browse to select an .hmg preset file containing the route's configuration that you want to apply to the current system.

   After a file is selected, you warning message appears in the view pane.
2. Click the Import button to start importing.
3. After the upload is complete, the file is validated for the following:
   - correct file extension (.hmg)
   - correct JSON format
   - it must contain at least one route configuration
   - a route must have a source
   - route name, source name and destination name are required and route name must be unique
4. If an error occurs, an error message is displayed. If validation passes, then it starts applying the preset.
5. While the system is applying the preset, a message "Applying preset..." is displayed with a progress bar.
6. When complete, a message of "# routes created" is displayed.

Certificates

From the Certificates page, 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 page lists the Identity Certificates available on Media Gateway. 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).

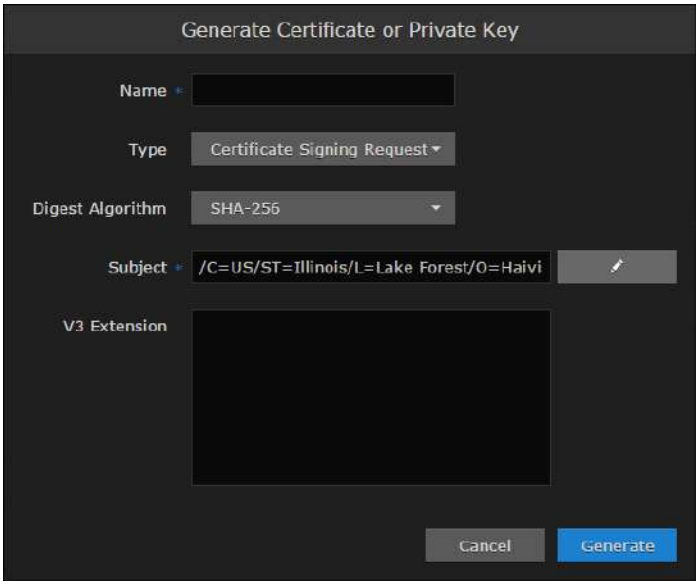
Generating a Certificate Signing Request

To generate a Certificate Signing Request (CSR):

1. Click the  icon and click ADMINISTRATION.
2. Click CERTIFICATES in the sidebar.

   The Certificates page lists any certificate signing requests generated on Media Gateway. The active certificate is indicated with a blue check.
3. Click the Generate button.
4. On the Generate Certificate or Private Key dialog:
   a. Type in a name for the certificate.
   b. Make sure the Type is Certificate Signing Request and fill in the remaining fields. See "Certificate Settings" on page 91.

c. For the subject, type in information about the device that the Identity Certificate represents. For more information, see "Subject" on page 92.



5. Click the Generate button.

NOTE

The generated CSR file needs to be sent to a Certification Authority to be signed. A copy of it is saved in the current administrator's home directory, or it can be copied and pasted from the CSR view. You can import the signed certificate back later by clicking on the Import button (using the same name as the CSR file).

6. Returning to the Certificates list, click the link for the generated CSR to open the file in another tab. Copy the contents (including both beginning and ending delimiters) and paste it into your Certificate Authority (CA) application.

   The CA returns an intermediate certificate (trust chain) and signed certificate (CRT).

TIP

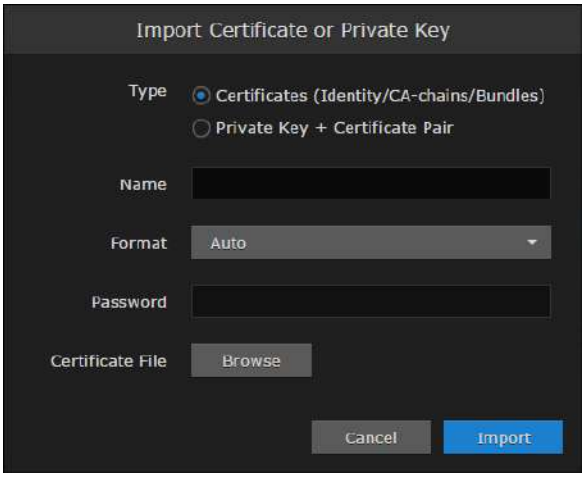
Keep in mind that there is a difference between importing a new certificate (that was generated externally) and importing a newly signed certificate whose request was previously generated on the Media Gateway and exported for signing.

Importing and Activating a Certificate

To import and activate a certificate:

1. Click the icon and click ADMINISTRATION.

2. Click CERTIFICATES in the sidebar.
3. Click the Import button.
4. On the Generate Certificate or Private Key dialog:
   a. Keep the default Type: Certificates (Identity/CA-chains/Bundles).
   b. Type in the certificate name and fill in the remaining fields. See "Certificate Settings" on page 91.
   c. If your certificate is encrypted, type in the password.
   d. Click Browse and select the CA-signed certificate (.crt extension) returned from the certificate request generated in the previous section.



5. Click Import.

   On the Certificates page, the newly imported certificate is added to the list and should have a green status LED. Click in the Active column to activate the certificate.
6. Click Reboot if you have changed the active certificate.

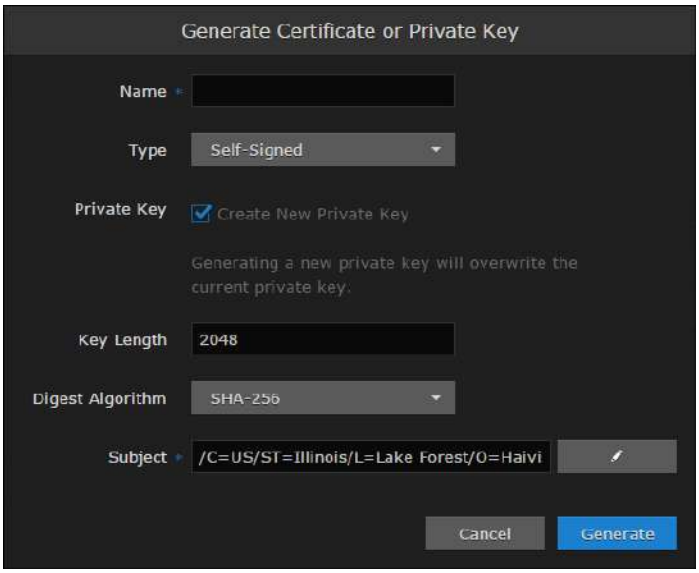
Generating and Importing a Private Key

To generate a private key:

1. Click the icon and click ADMINISTRATION.
2. Click CERTIFICATES in the sidebar.
3. Click the Generate button.
4. On the Generate Certificate or Private Key dialog:
   a. Type in a name for the certificate.
   b. For the Type, select Self-Signed.

c. Check the Create New Private Key checkbox.

d. Fill in the remaining fields. See "Certificate Settings" on page 91.



5. Click Generate.

CAUTION

Clicking Generate overwrites the current private key and renders unusable any certificates based on that key.

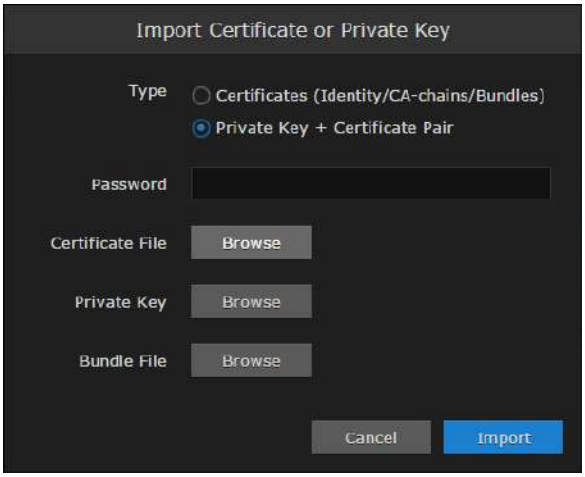
The new certificate is added to the Certificates list, and becomes the active certificate.

6. Click Reboot.

To import a Private Key:

1. Click the icon and click ADMINISTRATION.
2. Click CERTIFICATES in the sidebar.
3. Click the Import button.
4. On the Import Certificate or Private Key dialog:
   a. For the Type, select Private Key + Certificate Pair.
   b. Type in the password for the private key.

c. To update your security certificate, click Browse and select the new SSL Certificate and SSL Certificate (Private) Key, and optionally an SSL Intermediate Certificate Bundle file.



5. Click Import.

   On the Certificates page, the newly imported files are added to the list.

6. Click Reboot.

Certificate Settings

The following table lists the configurable Media Gateway 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.

Certificate Setting	Description
Generate Certificate or Private Key	
Name	Type in a unique name under which the certificate will be stored on the Media Gateway as well as listed on the Certificate page.
Type	Select the Signature Type: • Self-signed: The certificate will be generated and signed by the system, and the name will be added to the list of Identity Certificates. • 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): • SHA-256 • SHA-384 • SHA-512

Certificate Setting (Cont.)	Description (Cont.)
Subject	The Subject identifies the device being secured, in this case, the Media Gateway. The special value “auto” used with Generate sets the Subject Common Name to the device’s FQDN if DNS is set, or the IP address otherwise. Also, for self-signed certificates, the Subject Alternative Name extension is also set to FQDN, hostname, and IP Address of the device (there is no other method to set the Subject Alternative Name). Type in the subject in the form: "/C=US/ST=Maine..." where the most common attributes are: • /C Two Letter Country Name • /ST State or Province Name • /L Locality Name • /O Organization Name • /OU Organizational Unit Name • /CN Common Name TIP: For successful authentication, the Common Name in the certificate should be the IP address (by default) or domain name of the device.
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.
Import Certificate	
Type	Select the certificate type: • Certificates: (Identify/CA-chains/Bundles) • 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): • Auto: detected from the file extension • der: Distinguish Encoding Rules • pkcs #7 • pkcs #12
Password	If the imported certificate contains a password protected private key, type its password in this field. Leave this field empty if the file is not password-protected.
Certificate File	Select the file to upload

Update

Before upgrading a device, the update package must first be uploaded to the Media Gateway server. If you do not see the update package you want, check with your administrator and make sure that it is available.

IMPORTANT
Any update other than a maintenance release (for example, v1.1.*x*), requires a new license.

Downloading System Updates

To download system updates:

1. Log into the Haivision Download center at http://www.haivision.com/download-center.
2. Click the Software Upgrades link.
3. Download the Media Gateway upgrade package you wish to install.
4. Save the selected .zip file to your local computer or network.
5. Extract the update file from the .zip file using a zip file utility.

The system update comes in the form of a HaiBundle software package, which when loaded replaces the application on your device.

Related Topics

- "Viewing the Media Gateway Version Number" on page 76
- "Viewing the Status of a License" on page 76
- "Installing/Updating a Package (HaiBundle)" on page 93

Installing/Updating a Package (HaiBundle)

Updates are provided via a HaiBundle. You can find the latest HaiBundles on the Download Center as described in "Downloading System Updates" on page 93.

NOTE
Your system restarts after it installs the updates.

To install a HaiBundle:

1. Click the  icon and click ADMINISTRATION.

2. Click Update in the sidebar. The Update screen appears showing the currently installed version and build.
3. Click Browse.
4. Select the desired update bundle (.hai extension) and click Open.
5. Verify that the bundle listed is the one you want to install, and click Upload.
6. When the bundle has been uploaded, click Update.
7. When prompted, click OK to confirm. Your system restarts after it has installed the updates.

Related Topics

- "Downloading System Updates" on page 93

Accounts

To simplify setup and security, there are three built-in user accounts available: haiadmin, haioperator, and haiobserver.

Default credentials for each account are provided in the *Important Notice* document.

Viewing the Available User Accounts

User account information includes the name and role.

To view the available user accounts:

1. Click the icon and click ADMINISTRATION.
2. Click Accounts in the sidebar.

   The available accounts are listed in the view pane along with their current roles.

Field	Value
Account Name	The user name for the account. Built-in accounts set up at the factory include: • **haiadmin** — Built-in Administrator account. • **haioperator** — Built-in Operator account. • **haiobserver** — Built-in Observer account
Role	The role assigned to the account. Roles for built-in accounts are read-only. Available roles include: • **Administrator** — All access rights and administrator privileges. • **Operator** — All rights to create and configure routes. Does not include rights to the Administration page. • **Observer** — Read-only access to the system. Does not include the rights to the Administration page.

Related Topics

- "Changing an Account's Password" on page 95

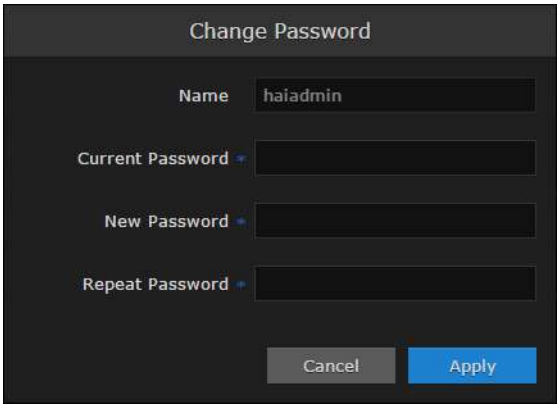
Changing an Account's Password

Any changes that you make to an account's password are persistent and are not overwritten during an update.

To change an account password from the web interface:

1. Click the icon on the toolbar and click Administration.

2. Click Accounts from the sidebar.
3. Click the Account Name whose password you want to change.
4. When the CHANGE PASSWORD dialog opens, enter your current password and a new password. Then re-enter your new password to confirm it.



5. Click Apply.

NOTE

The haiadmin password can also be changed in the Console UI. See "Changing the haiadmin Password" on page 107 for details.
The hvroot password can only be changed in the Console UI. See "Changing the Current User's Password" on page 106 for details.

Related Topics

- "Viewing the Available User Accounts" on page 95
- "Changing the haiadmin Password" on page 107
- "Changing the Current User's Password" on page 106

CHAPTER 5: Using the Console UI

The following content explains how to use the console user interface (UI) on a Media Gateway appliance. The Console UI provides a non-Web interface to perform basic system administration tasks and network tests.

NOTE

To connect to the Console UI directly, make sure the keyboard and monitor are correctly connected to the Media Gateway appliance. You can also access the Console UI using a secure shell connection (SSH).

Topics Discussed

Accessing the Console UI

Accessing the appliance Console UI requires administrator privileges and password.

To access the Console UI:

1. Connect a keyboard and monitor to the appliance, if applicable, and boot the appliance.

   -or-

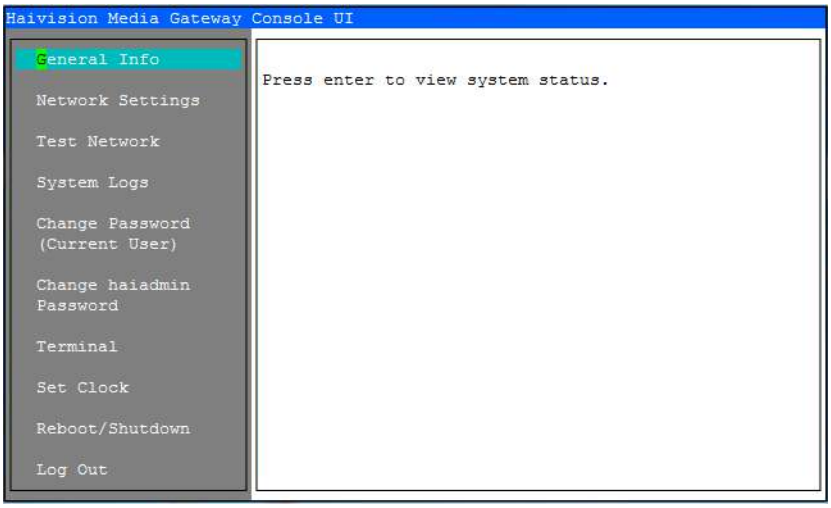
   Initiate a Secure Shell (SSH) connection to the IP address of the server using an SSH client (for example, PuTTY).

2. Log in using the hvroot username and password. Refer to the *Important Notice* document that accompanied your device for the default password.

NOTE

Use the TAB or ↑↓ (up and down arrow) keys to navigate the Console UI. *There is no mouse support.*

After you log in, the Console UI main screen appears.



The navigation sidebar (left pane) provides the menu/action items. The right pane displays a detailed view of the selected item. To control the Console UI:

- Use the TAB or ↑↓ (up and down arrow) keys to scroll through the navigation listings and text.
- Press ENTER to select the current item.
- To modify content, scroll to the line to change and, if necessary, backspace to delete the existing content and then type in your modifications.
- Press ENTER to save your changes or ESC to cancel and close the screen.

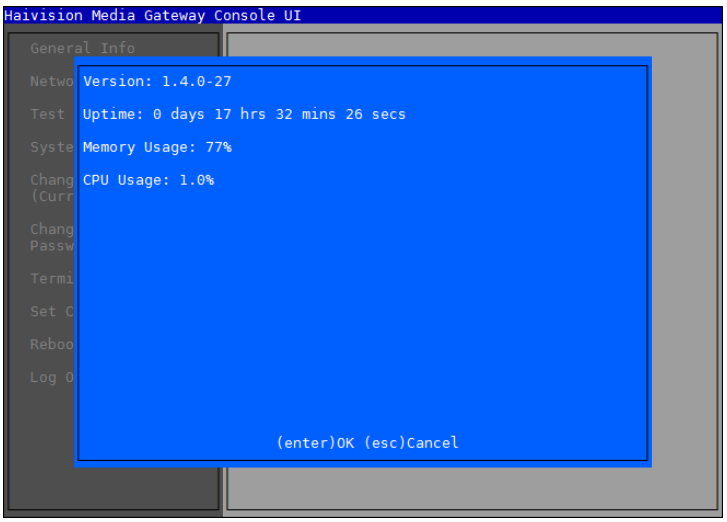
Showing General Information

The General Info screen displays system status information about the appliance, such as the firmware version, system uptime, memory usage, and CPU usage.

NOTE
This is a read-only screen.

To show the current system status:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight General Info.
2. Press the ENTER key. The General Information screen is shown.



3. When you are finished reviewing the information, press ENTER or ESC to exit to the main screen.

Related Topics

- "Accessing the Console UI" on page 98
- "Logging Out of the Console UI" on page 112

Editing Network Settings

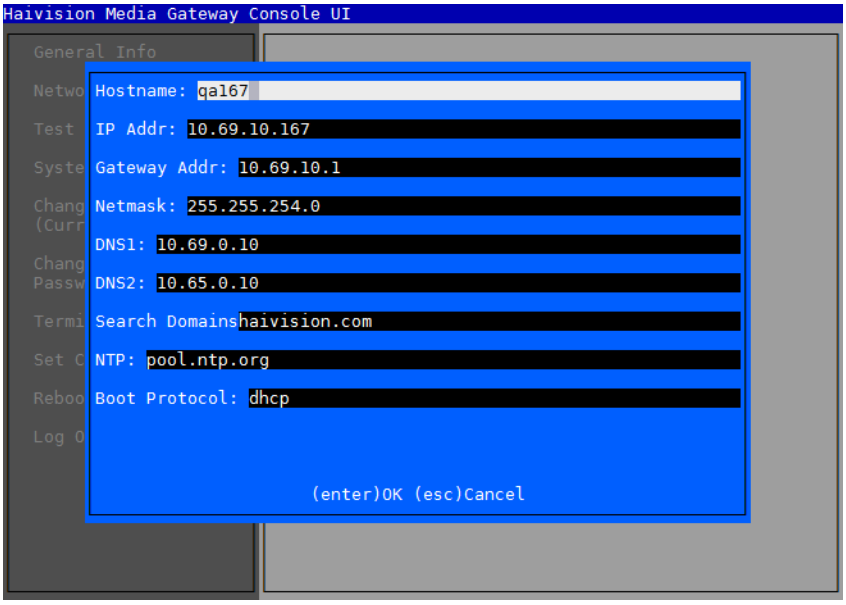
The Network Settings screen displays the following information for the unit:

- Hostname
- IP Address
- Gateway Address
- Netmask
- DNS Server Address 1
- DNS Server Address 2 (Must be set to a valid DNS address. Can use DNS1 if only one DNS server is available)
- Search Domains
- Network Time Protocol (NTP) Server Address *(optional)*
- Boot Protocol (DHCP or Static)

NOTE
These settings can also be changed in the web interface. See "Configuring the Network" on page 79 for details.

To change network settings:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight Network Settings.
2. Press the ENTER key.



3. To change a setting:
   - Use the TAB or ↑↓ (up and down arrow) keys to navigate to the field you want to change.
   - Use the DELETE/BACKSPACE key to delete the existing contents and then type in your modifications.
4. When finished editing the information, press ENTER to save your changes and exit to the main screen. Or, press the ESC key to exit without saving any changes.

Related Topics

- "Testing the Network Settings" on page 102
- "Configuring the Network" on page 79

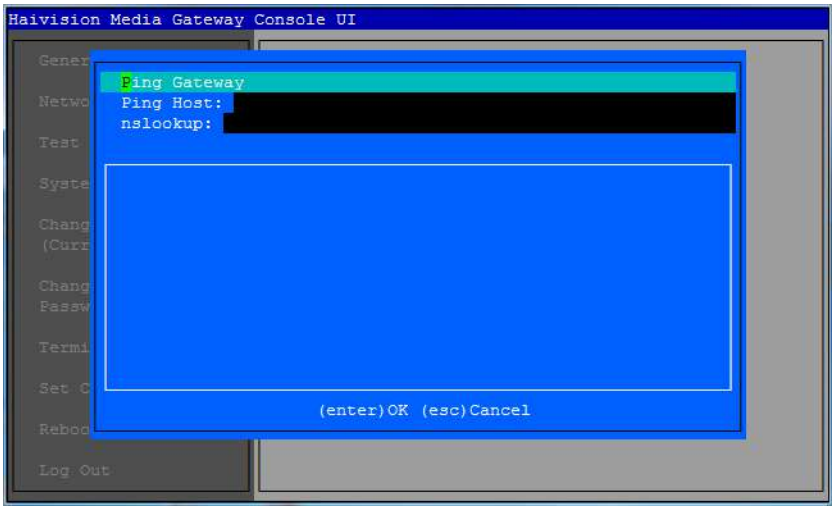
Testing the Network Settings

TIP

For descriptions of the network settings, please see the documentation that accompanied your appliance.

To test the network settings:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight Test Network.
2. Press the ENTER key.



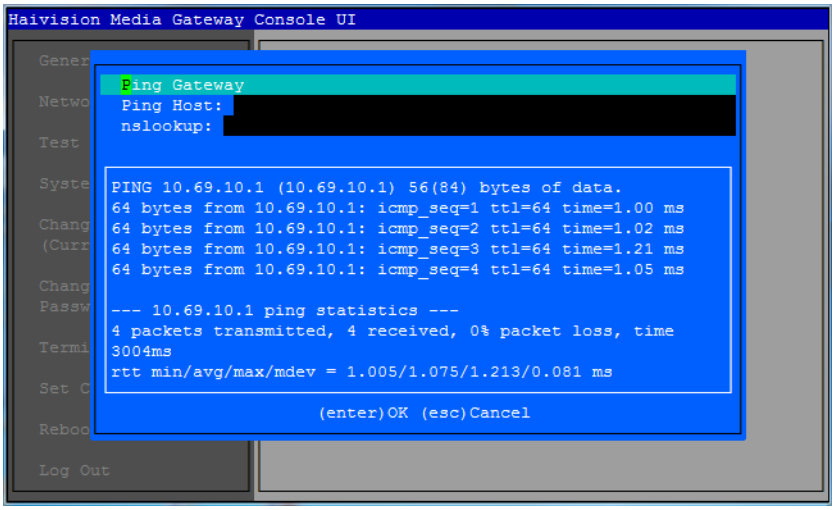
The Test Network screen provides four possible network setting tests:

Test	Description
Ping Gateway	Press ENTER to ping the defined gateway IP (that is, to send echo request packets).
Ping Host	Type in the host IP address and press ENTER.
nslookup	(Name Server Lookup) Type in a Fully Qualified Domain Name (FQDN) and press ENTER.
Connect to web	Type in a valid URL and press ENTER.

3. To perform a network test:
   - Use the TAB or ↑↓ (up and down arrow) keys to navigate to the test you want to perform.

- In the text entry field for your selected test, use the DELETE/BACKSPACE key to delete any existing contents, then type in your modifications, and press ENTER.

An example of the Ping Gateway test results is shown below.



4. When finished, press ESC to exit to the main screen.

Related Topics

- "Editing Network Settings" on page 100

Viewing System Logs Available through the Console UI

The Media Gateway system log provides useful information regarding installations, packages, plug-ins, console sessions, authentications, kernel messages, and database errors.

TIP

System logs are also accessible via the Media Gateway web interface. See "Viewing Reports (Logs)" on page 67 for details.

To view a system log:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight System Logs.
2. Press the ENTER key.

The System Logs screen provides five possible systems logs to review:

Log	Description
Upgrade Log	Provides log entries regarding installations, packages, plugins, and so forth.
Console UI Log	Provides log entries console sessions, authentications, boot protocol, and the like.
Haivision Log	Provides log data.

Log	Description
Linux Messages	Provides kernel messages regarding initialization, process, commands, among other things.
Application Startup Log	Provides information regarding application startup.

3. To review a particular log, use the TAB or ↑↓ (up and down arrow) keys to navigate to the log you want to view.
4. Press ENTER, and the log file is displayed on the screen.
5. When finished, press ESC to exit to the main screen.

Related Topics

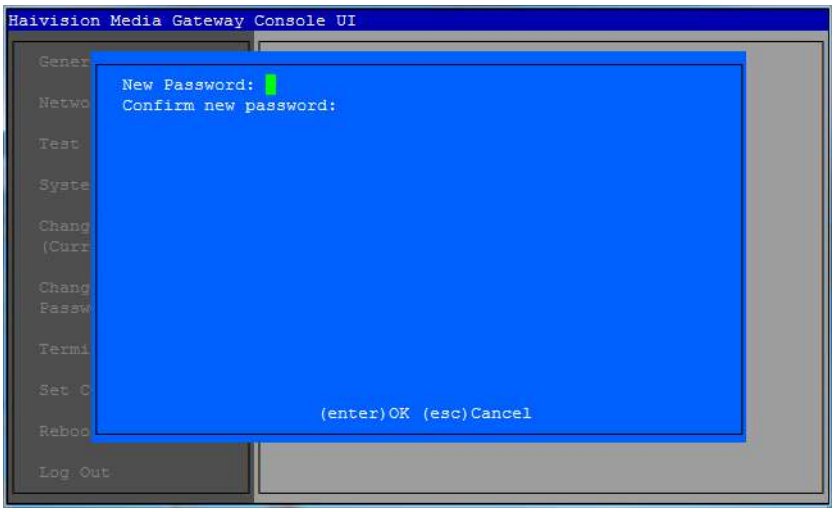
- "Viewing Reports (Logs)" on page 67

Changing the Current User's Password

At this time, the only user that can remote login to the device using secure shell (ssh) is the hvroot user. Use the following procedure to change the password for hvroot.

To change the password for the current user:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight Change Password (Current User).
2. Press the ENTER key.



3. Type in the new password.
4. Press TAB or the ↓ (down arrow) and type the password again in the Confirm new password line.
5. Press ENTER. Upon success, the prompt confirms that the password has been changed and then returns to the main screen.

Related Topics

- "Accessing the Console UI" on page 98

Changing the haiadmin Password

TIP

The haiadmin password can also be changed in the Media Gateway web interface. See "Changing an Account's Password" on page 95 for details.

To change the haiadmin password:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight Change haiadmin Password.
2. Press the ENTER key.

3. Type in the new password.
4. Press TAB or the ↓ (down arrow) and type the password again in the Confirm new password field.
5. Press ENTER. Upon success, the prompt confirms that the password has been changed and then returns to the main screen.

Related Topics

- "Changing the Current User's Password" on page 106

Opening a Console UI Terminal Window

To open a terminal window:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight Terminal.
2. Press the ENTER key.

3. When the bash shell opens, enter your commands.
4. When finished, press CTRL+X to exit to the main screen.

Related Topics

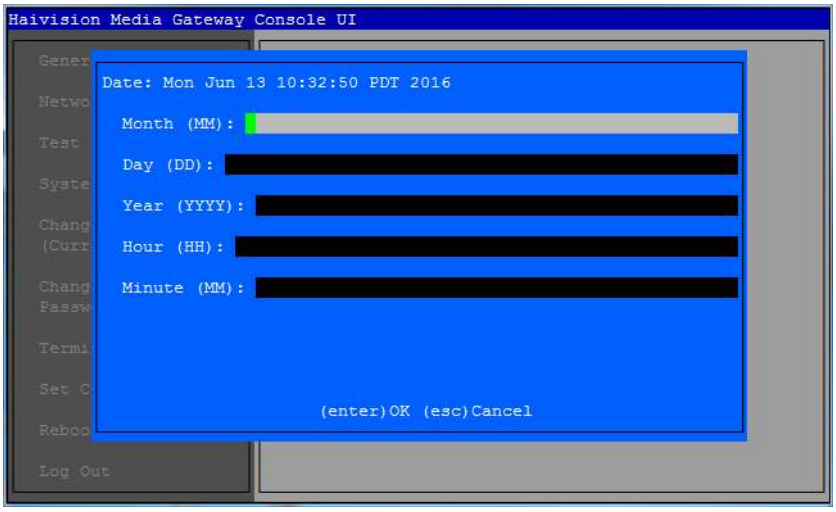
- "Accessing the Console UI" on page 98
- "Logging Out of the Console UI" on page 112

Setting the Clock

To change the time and date:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight Set Clock.
2. Press the ENTER key.

3. Press ENTER again to select Set Clock.
4. Enter the appropriate values. Press TAB or the ↓ (down arrow) to move between the fields.



5. Press ENTER to set the new time and date.

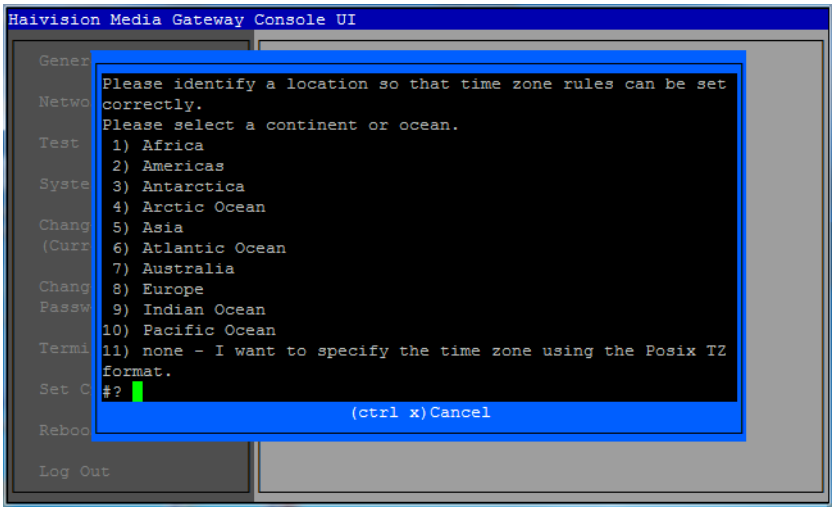
Related Topics

- "Setting the Timezone" on page 110

Setting the Timezone

To change the timezone:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight Set Clock.
2. Press the ENTER key.
3. Press TAB or the ↓ (down arrow) to select Set Timezone.
4. Press ENTER.
5. Make your timezone selection and press ENTER.



NOTE

If you choose the option to specify the time zone using the POSIX TZ format, the format is:

TZ = local_timezone+/- hours to UTC.
For example, TZ='CST-6'

For more information, refer to the following article:
https://en.wikipedia.org/wiki/Tz_database#Names_of_time_zones

Related Topics

- "Setting the Clock" on page 109

Rebooting or Shutting Down

To reboot or shut down:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight Reboot/Shutdown.
2. Press the ENTER key.

3. Use the ↑↓ (up and down arrow) keys to highlight either Reboot or Shutdown as appropriate.
4. Press ENTER.
5. When prompted to confirm, press either:
   - Y for yes
   - N to cancel

   After confirming your selection, the system either shuts down or reboots (as appropriate). You are then automatically logged off and your secure shell (ssh) connection is closed.

NOTE
If you selected to reboot, you can reconnect the secure shell (ssh) and log into the device once the system has restarted.

Related Topics

- "Accessing the Console UI" on page 98

Logging Out of the Console UI

To log out of the Console UI:

1. In the navigation sidebar, use the ↑↓ (up and down arrow) keys to highlight Log out.
2. Press the ENTER key.

3. At the prompt, type Y to confirm or N to cancel.
4. Press ENTER.

   After logging out, you are redirected to the login screen

Related Topics

- "Accessing the Console UI" on page 98

APPENDIX A: Troubleshooting

Known Issues and Solutions

To view a list of additional known issues, solutions, and recommended practices, visit:

http://www.haivision.com/support/knowledgebase/

☒ Erratic Behavior after a Recent Update

✓ If you have recently updated your web-based interface *software*, it is possible that your browser's cache is pointing to an older file. **Clear your browser's cache to ensure that the interface accesses the most recently installed files**.

☒ Cannot start the Web-Based Interface

✓ To start the web-based interface, in your browser enter the *base URL*. For example:

http://127.0.0.1

☒ The Web-Based Interface Login isn't Working

✓ Make sure the CAPS LOCK key is not ON.

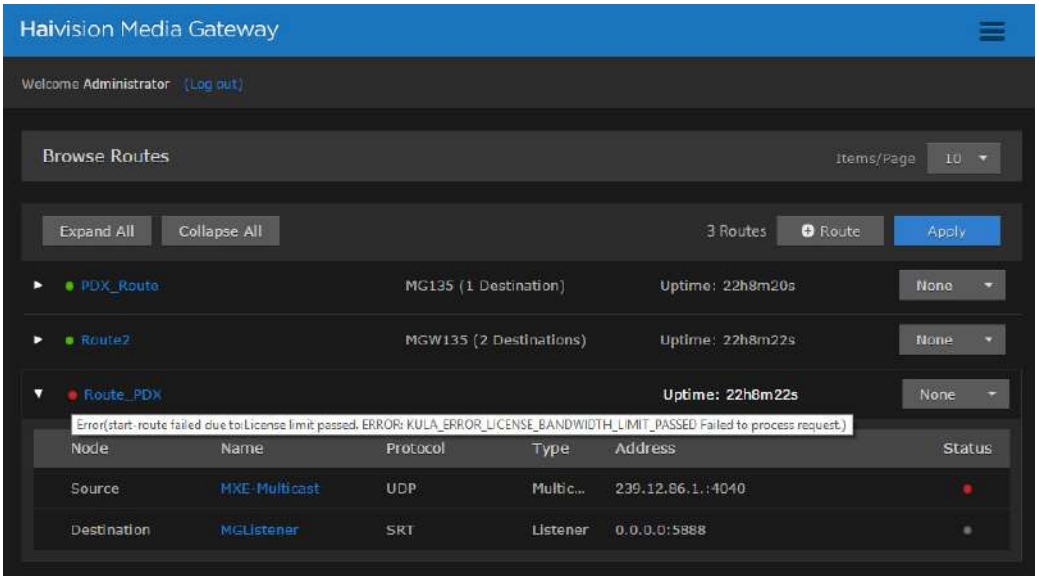
✓ Make sure that you have cookies enabled in your browser.

☒ Identifying your Software Version from the Interface

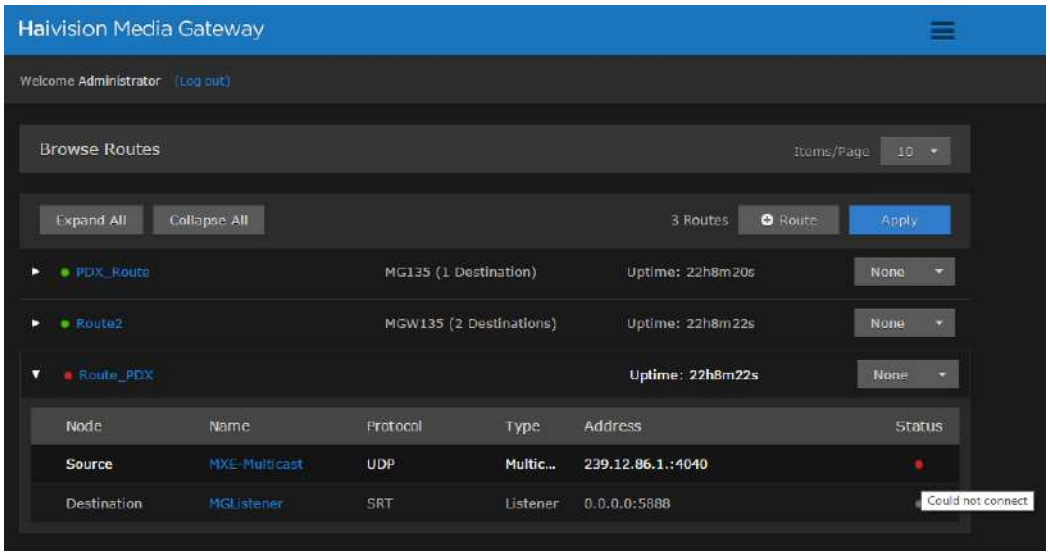
✓ To view the current release number for your Media Gateway installation, click the  icon and select ABOUT MEDIA GATEWAY.

☒ Status Indicator is not Green

✓ Verify that your license has adequate bandwidth.



✓ Hover your mouse cursor over the status indicator. A popup will appear to provide some context as to why there is an error.



☒ Error Message states Failed to receive segment: cross domain request denied.

✓ Verify that you have entered the cross-domain address correctly. See “Pairing the Devices” on page 71.

Technical Support and Updates

Refer to your Media Gateway documentation suite for instructions on setting up and using the Haivision Media Gateway. You may download the PDF version of the documentation, as well as the Release Notes and software from our Download Center at http://www.haivision.com/download-center/.

For more information, visit Haivision Technical Support through the Support Portal on our website at: http://www.haivision.com/support/. Or contact us using the phone numbers and email addresses listed under “Audience” on page 8.

APPENDIX B: Glossary of Terms

Glossary

AES	Advanced Encryption Standard. A specification for the encryption of electronic data established by the U.S. National Institute of Standards.
AAC	Advanced Audio Coding (AAC). A standardized, lossy compression and encoding scheme for digital audio. Designed to be the successor of the MP3 format, AAC generally achieves better sound quality than MP3 at similar bitrates.
AAC-LD	AAC Low Delay. An audio compression standard designed to combine the advantages of perceptual audio coding with the low delay necessary for two-way communication. It is closely derived from the MPEG-2 Advanced Audio Coding (AAC) standard.
API	Application Programming Interface. For the purposes of this document, API refers to the collection of entities, operations and supporting materials provided with the API.
aspect ratio	The proportion of width to height of an image or screen.
audio bitrate	The number of bits used per unit of time to represent an audio stream. Measured in kilobits per second (kbps).
audio gain	Measures of the ability of a circuit (often an amplifier) to increase the power or amplitude of a signal from the input to the output, by adding energy to the signal converted from some power supply. Measured in decibels (dB).
AVC	Advanced Video Coding. A standard for video compression, used for the recording, compression, and distribution of high definition video.
B-frame	Contains difference information from the preceding and following I- or P-Frame within a Group of Pictures (GOP). Backward prediction enhances encoding decisions for moving objects, but requires significant increase in buffer size. Typically, most broadcast-quality applications use IBBP to optimize video quality with compression efficiency.
baseline profile	Targeted at light applications such as video conferencing or playback on mobile devices with limited processing power.

CABAC	Context-based Adaptive Binary Arithmetic Coding. More advanced and gives a better bit-rate-to-quality economy at the cost of higher processing power. For higher-quality applications such as large-format web video.
CALVC	Context-based Adaptive Variable Length Coding for lower-quality applications.
cascade	The set of outputs that make up adaptive bit rate groups.
CBR	Constant Bit Rate. The encoder/transcoder will generate a constant number of bits over a period of time.
CDN	Content Delivery Network. A content delivery network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content.
channel	A single video input into an encoder/transcoder.
CLI	Command Line Interface. a means of interaction with a computer program where the user (or client) enter lines of text to issue commands to the program.
Closed Captioning	The act or process of including text as the transcription of the audio portion to a digital video stream or program. NOTE: When closed captioning information is encoded in the MPEG-2 data stream, only the decoder has access to the data; there is no standard for transmitting the data to a display monitor separately.
closed captions	The actual text that appears on the screen during closed captioning.
cloud encoder	An encoder that does not include any video capture cards. A cloud encoder requires the use of a source encoder streaming RTMP as input.
Codec	enCOde/DECode; a device or computer program capable of encoding and/or decoding a digital data stream or signal. A codec is a particular technology or method used to compress and electronic signal, such as a video or audio recording.
color space	Defines colors as a function of the absolute reference frame, color spaces, along with device profiling, to allow reproducible representations of color, in both analogue and digital representations.
CRADA	Cooperative Research and Development Agreement. a written agreement between a private company and a government agency to work together on a project.
cURL	Command line tool for getting and sending files using the URL syntax.
data field	A data field can either directly display the text from a data table or it can display an image or other media asset that the data table contains.

data panel	A data panel is a special grouping of data fields that can be used to aid when creating content that displays multiple rows of data in a table-like format.
DEB	DEB is the extension of the Debian Software Package format and the most often used name for such binary packages.
deinterlace	The process to convert interlaced video back into its non-interlaced form. Employs complex algorithms; however, results vary.
DVR	Digital Video Recorder. A device or application software that records video in a digital format to a disk drive, USB flash drive, SD memory card, SSD or other local or networked mass storage device.
directory rollover	For HLS Akamai HD network distribution. When this box is checked, it limits the number of .ts segments to 2000 before rolling over to a new directory.
encoder/transcoder	A computer or appliance that takes video and audio input or digital video and audio input and encodes or transcodes to a digital format.
endpoint	A URI that points to a function or operation provided by the API, e.g., /apis/demos.
ECS	Encoder Communication Server is a program running on the KulaByte Transcoder encoder system that manages one or more encoder processes. This manager of encoder processes also uses a REST server to expose its system encoder processes.
event	A stream or streams that are to be broadcast or archived. An event is usually broadcast live.
FEC	Forward Error Correction.
frame rate	The video frame rate per second. The number of still images that are displayed in a given time interval to provide the illusion that the images are moving. A typical frame rate is 24 frames/second. (PAL uses 25fps while NTSC uses 29.97). Each picture of a video – either a frame or a field – is partitioned into as many macroblocks as necessary to cover the picture area. These macroblocks serve as the basic element for operations such as spatial/temporal compression, motion compensation, and re-encoding.
Furnace	The Haivision IPTV media system.
GOP	Group of Pictures. Specifies the order in which intra- and inter-frames are arranged.
GUID	Globally Unique Identifier or UUID (Universally Unique Identifier). A 128-bit integer number that identifies resources. The format is a defined sequence of 32 hex digits grouped into chunks of 8-4-4-4-12.
H.264	A codec that is intended to serve a wide range of applications – from highly compressed, low-frame-size videos to large format, cinema-quality videos.

H.265	*See HEVC.*
HDCP	High-bandwidth Digital Content Protection (HDCP; commonly, though incorrectly, referred to as High-Definition Copy(right) Protection) is a form of digital copy protection developed by Intel Corporation to prevent copying of digital audio and video content as it travels across connections.
HDS	HTTP Dynamic Streaming
HE-AAC	High Efficiency Advanced Audio Coding
HEVC	High Efficiency Video Coding. Also known as H.265 and MPEG-H Part 2. HEVC is a draft video compression standard, currently under development as a successor to H.264/MPEG-4 AVC (Advanced Video Coding).
high profile	Most efficient of the top three profiles. Packs more quality into a given bit rate. Hardest to process. Originally intended for high-definition applications such as Blu-Ray, however becoming popular for web-video applications due to the increase in processing power.
HLS	HTTP Live Streaming. An HTTP-based media streaming communications protocol created by Apple® Inc. as part of their QuickTime® and iPhone® software systems.
HTTP Dynamic Streaming	HDS, Enables on-demand and live adaptive bitrate video delivery of standards-based MP4 media over regular HTTP connections.
I-frame	Intra-Coded Picture, usually referred to as a *reference frame*. An I-Frame contains the full image of the picture (that is, it is not a delta).
input presets	New set of input settings grouped under a central theme, which can be saved and recalled for later use.
interlace	A method to reduce transmission bandwidth where frames are divided into two consecutive fields: one of all even lines and the other of all odd lines. Leverages the fact that analog devices scan serially to render the picture faster.
JITC	Joint Interoperability Test Command. Conducts testing of national security systems and information technology systems hardware, and software. Services include developmental, conformance, interoperability, operational and validation testing.
JMIT	JITC Motion Imagery Tool. Ensures that motion imagery systems conform to the JITC standards.
key frame	Full frames directly derived from the original source without the use of references to other frames within the video.
KLV	Key Length Value. Refers to metadata packets. A data encoding standard, often used to embed information in video feeds. Items are encoded into Key-Length-Value triplets, where key identifies the data, length specifies the data's length, and value is the data itself.

Kraken	The Haivision real-time stream-based video transcoder.
level	A restriction on the rate of chunks the decoding process could run into. The higher the level the higher this restriction is set. This translates into a frame size and frame rate combination restriction.
LATM	Low Overhead Audio Transport Multiplex (LATM). An interleaved multiple stream version of a LOAS.
LOAS	Low Overhead Audio Stream (LOAS). A self-synchronizing format that encapsulates not only AAC, but any MPEG-4 audio compression scheme such as Twin VQ and ALS.
lossless compression	Decompression process which results in a file identical to the original.
lossy compression	Process by which the data is reduced in such a manner that it takes significantly less space than lossless compression alone, simply by discarding some, possibly most of the original data. The trick is to discard in such a way that the missing information will not be obvious.
MAC address	Media Access Control address. A unique identifier assigned to a network interface card, usually assigned by the network card manufacturer.
main profile	More capabilities than Baseline, better efficiency than baseline, but comes at the cost of a relatively higher CPU overhead. Usually used in medium-quality web video applications.
method	For the purposes of this document, this refers to the HTTP methods GET, POST, PUT, or DELETE.
MPEG TS	MPEG Transport Stream, MTS, or TS. A standard format for transmission and storage of audio, video, and Program and System Information Protocol (PSIP) data. It is used in broadcast systems such as DVB, ATSC, and IPTV.
MTU	Maximum Transmission Unit. Specifies the maximum allowed size of IP packets for the encoded or transcoded stream.
NDPP	Network Device Protection Profile. U.S. Government Approved Protection Profile
NIC	Network Interface Card.
NTP	Network Time Protocol is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
P-frame	Predicted Picture or delta-frame, stores only the changes in the image from the previous frame. This minimizes the storage space needed thereby improving compression rates.

payload	Sometimes referred to as the actual or body data. It is the *cargo* of a data transmission, or the part of the transmitted data which is the fundamental purpose of the transmission.
PID	Packet Identification.
PIN	Personal Identification Number.
PMT	Program Map Table, a collection of PIDs available in a transport stream.
preset	A preset is the defined settings for an event.
profiles	A series of features sets aimed at different applications. Most common are Baseline, Main, and High.
property expression	When you create a data field, a binding expression is automatically generated for you that links the data field to a value in a data table. You can edit the expression for a data field or add a new expression for a text field with the Edit Expression dialog.
resolution	The stream output resolution, that is, the number of lines per frame and pixels per line to be encoded/transcoded.
REST	Representational State Transfer. A style of software architecture for distributed hypermedia systems.
RTMP	Real Time Messaging Protocol. A protocol for streaming audio, video and data over the Internet, used primarily between an Adobe® Flash player and a server.
session	New set of recording attributes grouped under a central theme, which can be saved and recalled for later use.
source encoder	This is an encoder that encodes from a source to a flash server (FMS). This source encoder's stream is then ingested by a cloud encoder.
SRT	Secure Reliable Transport. SRT is a transport technology that optimizes streaming performance across unpredictable networks like the Internet. Packet loss and jitter exist over almost any network connection. Bandwidth on readily-provisioned Internet connections fluctuates due to congestion. SRT provides end-to-end security, resiliency, and dynamic endpoint adjustment based on real-time network conditions to deliver the best video quality at all times.

ST	Security Target. An ST defines information assurance security and functional requirements for the given information system product, which is called the Target of Evaluation (TOE). An ST is a complete and rigorous description of a security problem in terms of TOE description, threats, assumptions, security objectives, security functional requirements (SFRs), security assurance requirements (SARs), and rationales. The SARs are typically given as a number 1 through 7 called Evaluation Assurance Level (EAL), indicating the depth and rigor of the security evaluation, usually in the form of supporting documentation and testing, that the product meets the SFRs.
stream bundling	Stream Bundling establishes a single network connection to send all RTMP adaptive bitrate streams to a CDN. Limelight and Ustream require the use of stream bundling, while Akamai recommends against it. Note: Applies to RTMP streams only.
SVC	Scalable Video Coding. An extension of the video compression standard H.264/MPEG-4 AVC.
time shifting	The recording of programming to a storage medium to be viewed or listened to at a time more convenient to the consumer. Depending upon the digital video recorder (DVR), it may be possible to start playback before the recording is complete.
timecode	A sequence of numeric codes generated at regular intervals by a timing synchronization system.
ToS	Type of Service. Specifies the desired quality of service (QoS). This value is assigned to the Type of Service field of the IP Header for the outgoing streams.
transcoding	The direct digital-to-digital data conversion of one encoding to another.
TS Segments	Transport Stream segments, a delivery format for audio-video.
TTL	Time-to-Live for stream packets. Specifies the number of router hops the stream packet is allowed to travel/pass before it must be discarded.
UI	User interface. Provides effective operation and control of the machine, and feedback from the machine to aid the operator in making decisions
Universally Unique Identifier	UUID, is a 128-bit integer number that identifies resources. The format is a defined sequence of 32 hex digits grouped into chunks of 8-4-4-4-12.
URI	Uniform Resource Identifier. The Web naming/addressing technology that uses short strings to identify resources.
URL	Uniform Resource Locator. A specific type of URI. For the purposes of this document, URI and URL are used interchangeably.

VBR	Variable Bit Rate. VBR streams vary the amount of output data per time segment. VBR allows a higher bitrate to be allocated to the more complex segments of media streams while less space is allocated to less complex segments.
video bitrate	The number of bits used per unit of time to represent a video stream. Measured in kilobits per second (kbps).
VoD	Video on Demand. An interactive technology that allows users to select and view programming in real time or download programs and view them later.
XML entity	An XML opening and closing tag in combination with its payload. For example, the “demo” entity refers to: <demo> <id>myID</id> <name>myName</name> <value>myValue</value> </demo>
XML tag	A named XML entity, for example, <demo/>.
YC_BC_R or $Y'C_BC_R$	A family of color spaces used as a part of the color image pipeline in video and digital photography systems.

APPENDIX C: Warranty

Haivision One (1) Year Limited Warranty

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

EXCLUSIONS AND LIMITATIONS

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

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

This warranty does not apply:

(a) to cosmetic damage, including but not limited to scratches, dents and broken plastic on ports;

(b) to damage caused by accident, abuse, misuse, flood, fire, earthquake or other external causes;

(c) to damage caused by operating the product outside the permitted or intended uses described by Haivision;

(d) to a product or part that has been modified to alter functionality or capability without the written permission of Haivision; or

(e) if any Haivision serial number has been removed or defaced.

TO THE EXTENT PERMITTED BY LAW, THIS WARRANTY AND REMEDIES PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, REMEDIES AND CONDITIONS, WHETHER ORAL OR WRITTEN, STATUTORY, EXPRESS OR IMPLIED. AS PERMITTED BY APPLICABLE LAW, HAIVISION SPECIFICALLY DISCLAIMS ANY AND ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRAN-

TIES 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 http://www.haivision.com/support-portal-home. 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.

Haivision Software End-User License Agreement

READ BEFORE USING

THE SOFTWARE PROGRAMS ARE PROTECTED BY NATIONAL AND INTERNATIONAL COPYRIGHT LAWS AND TREATIES. READ THE TERMS OF THE FOLLOWING END USER (SOFTWARE) LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE PRODUCT. BY USING THE PRODUCT, 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 INSTALL OR USE THE LICENSED SOFTWARES.

1. DEFINITIONS

1.1 Entitlement. The collective set of applicable documents authorized by Haivision Network Video or its affiliate Haivision (collectively "Haivision) evidencing your obligation to pay associated fees (if any) for the license, associated Services, and the authorized scope of use of Licensed Software under this Agreement.

1.2 You (or Your). The individual or legal entity specified in the Entitlement, or for evaluation purposes, the entity performing the evaluation.

1.3 License Fee. License Fee shall mean the consideration paid to Haivision for use of the Licensed Software. The License Fee is part of the price paid for the relevant Product.

1.4 Licensed Software. Licensed Software shall mean the executable version of Haivision's computer software, program or code, in object code format (specifically excluding source code), together with any related material including, but not limited to the Reference Manuals or database schemas provided for use in connection with the Licensed Software and including, without limitation, all Upgrades through the date of installation.

1.5 Reference Manuals. Reference Manuals shall mean the most current version of the documentation for use in connection with the Licensed Software provided by Haivision to You.

1.6 Updates. Updates shall mean any periodic software releases, additions, fixes, and enhancements thereto, release notes for the Licensed Software and related Reference Manuals, (other than those defined elsewhere in this section as Upgrades) which have no value apart from their operation as part of the Licensed Software and which add minor new functions to the Licensed Software, but none so significant as to warrant classification as an Upgrade, which may be provided by Haivision to fix critical or non-critical problems in the Licensed Software on a scheduled, general release basis. Updates to the Licensed Software ("Version") are denoted by number changes to the right of the decimal point for a version and revision number (for example going from 2.0.0 to 2.1.3).

1.7 Upgrades. Upgrades shall mean any modification to the Licensed Software made by Haivision, which are so significant, in Haivision's sole discretion, as to warrant their exclusion under the current license grant for the Licensed Software. Upgrades of Licensed Software are denoted by number changes to the left of the decimal point for a release number (for example going from 2.0 to 3.0).

2. RIGHTS GRANTED, RESTRICTIONS AND SUPPORT

2.1 License to Use.

(a) Subject to the terms and conditions set forth herein and subject to the terms of your Entitlement, Haivision hereby grants to You a non-exclusive, personal, limited and nontransferable right and license to use the Licensed Software in accordance with the terms of this Agreement. This license is granted to You and not, by implication or otherwise, to any parent, subsidiary or affiliate of Yours without Haivision's specific prior written consent. This license is for the limited use of the Licensed Software by You for the purpose of creating, managing, distributing and viewing IP Video assets. This license does not grant to You the right to use any Licensed Software in connection with any public broadcasting or broadcasting for home

or residential purposes, or any license for content whatsoever. The license and rights granted to You in this Section (2.) do not include the right to sublicense to distributors, resellers and other third parties any of the rights granted to You in this Section (2.). All rights not expressly granted You in this Agreement are reserved to Haivision and no implied license results from this license.

2.2 Restrictions.

(a) Reproduction. You shall not copy, distribute, reproduce, use or allow access to any of the Licensed Software, except as explicitly permitted under this Agreement. You shall not modify, adapt, translate, export, prepare derivative works from, decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the Licensed Software or any internal data files generated by the Licensed Software, or use the Licensed Software embedded in any third party hardware or software. You shall also not use the Licensed Software in an attempt to, or in conjunction with, any device, program or service designed to circumvent technological measures employed to control access to, or the rights in other work protected by copyright laws. You shall not remove, modify, replace or obscure Haivision's copyright and patent notices, trademarks or other proprietary rights notices affixed to or contained within any Licensed Software. No right is granted hereunder for any third party who obtains access to any Licensed Software through You to use the Licensed Software to perform services for third parties.

(b) Ownership. The Licensed Software is conditionally licensed and not sold. As between the parties, Haivision and/or its licensors owns and shall retain all right, title and interest in and to all of the Licensed Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein, and nothing in this Agreement shall be deemed to transfer to You any ownership or title to the Licensed Software. You agree that it will not remove, alter or otherwise obscure any proprietary rights notices appearing in the Licensed Software. All Haivision technical data and computer software is commercial in nature and developed solely at private expense.

3. TERM AND TERMINATION

3.1 Term. The license and service term are set forth in your Entitlement(s). Additionally, this Agreement may be terminated without cause by You upon thirty (30) days written notice to Haivision.

3.2 Termination for Breach. Your rights under this Agreement will terminate immediately without notice from Haivision if You materially breach it or take any action in derogation of Haivision's rights to Software. Haivision may terminate this Agreement should any Software become, or in Haivision's reasonable opinion likely to become, the subject of a claim of intellectual property infringement or trade secret misappropriation.

3.3 Termination; Effect; Survival. Upon the termination of this Agreement for any reason: (a) all license rights granted hereunder shall terminate; (b) You shall immediately pay to Haivision all amounts due and outstanding as of the date of such termination or expiration; and (c) You shall return to Haivision all Licensed Software and all Haivision Confidential Information not otherwise required under the terms of this Agreement or certify that all such Licensed Software and Confidential Information have been destroyed. Notwithstanding any termination of this Agreement, the following provisions of this Agreement shall survive for the relevant period of time set forth therein, if any: Sections 2.2, 4.1, 4.2, and 6.

4. REPRESENTATIONS, DISCLAIMER AND LIMITATION OF LIABILITY

4.1 Haivision Warranty.

(a) Haivision warrants that the Licensed Software will operate substantially in accordance with the Reference Manuals provided for a term of ninety (90) days (the "Warranty Period") after its delivery date. As Your sole and exclusive remedy for any breach of this warranty, Haivision will use its commercially reasonable efforts to correct any failure of the Licensed Software to operate substantially in accordance with the Reference Manuals which is not the result of any improper or unauthorized operation of the License Software and that is timely reported by You to Haivision in writing within the Warranty Period, provided that in lieu of initiating commercially reasonable efforts to correct any such breach, Haivision may, in its absolute discretion, either (i) replace the Licensed Software with other software or technology which substantially conforms to the Reference Manuals or (ii) refund to You a portion of the fee paid for the relevant Product, whereupon this Agreement shall terminate. This warranty shall immediately terminate if You or any third party makes or attempts to make any modification of any kind whatsoever to the Licensed Software.

(b) All proprietary Hardware, if any, will be subject to the then current warranty terms of Haivision. All non-proprietary Hardware, if any, is sold "AS IS"; however, to the extent that Haivision has the legal right to do so, Haivision hereby transfers to You any and all warranties made by Haivision's vendors to Haivision with respect to such non-proprietary Hardware which was sold by Haivision or the Reseller to You, provided that You expressly acknowledge and agree that Haivision disclaims any and all liability in connection with any such non-proprietary Hardware, as set forth in Section 4.2(b) of this Agreement.

4.2 Warranty Disclaimers.

(a) THE EXPRESS WARRANTIES SET FORTH IN SECTION 4.1(a) ABOVE IN RESPECT OF THE LICENSED SOFTWARE ARE IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, OR STATUTORY, REGARDING THE LICENSED SOFTWARE, OR ITS OPERATION, FUNCTIONALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS (ALL OF WHICH ARE DISCLAIMED). HAIVISION DOES NOT WARRANT THAT ANY OF THE LICENSED SOFTWARE WILL MEET ALL OF YOUR NEEDS OR REQUIREMENTS, OR THAT THE USE OF ANY OF THE LICENSED SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL ERRORS WILL BE DETECTED OR CORRECTED.

(b) THE EXPRESS WARRANTIES SET FORTH IN HAIVISION'S WARRANTY TERMS IN RESPECT OF HAIVISION PROPRIETARY HARDWARE ARE IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, OR STATUTORY, REGARDING ANY SUCH PROPRIETARY HARDWARE, OR ITS OPERATION, FUNCTIONALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ALL NON-PROPRIETARY HARDWARE SOLD BY HAIVISION OR THE RESELLER TO YOU IS SOLD "AS IS" EXCEPT FOR HAIVISION'S AGREEMENT TO TRANSFER TO YOU ANY WARRANTY GIVEN TO IT BY ANY VENDOR FROM WHOM SUCH HARDWARE WAS PURCHASED FOR RESALE TO YOU HEREUNDER IN ACCORDANCE WITH THE PROVISIONS OF SECTION 4.1(b), AND HAIVISION DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, OR STATUTORY, REGARDING ANY SUCH NON-PROPRIETARY HARDWARE, OR ITS OPERATION, FUNCTIONALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

4.3 Liability Limitation. IN NO EVENT SHALL HAIVISION OR ITS OFFICERS, EMPLOYEES, AGENTS, REPRESENTATIVES, MEMBERS OF HAIVISION, NOR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED SOFTWARE, BE LIABLE TO YOU, YOUR CUSTOMERS OR TO ANY OTHER THIRD PARTY FOR

CONSEQUENTIAL, INDIRECT, INCIDENTAL OR SPECIAL DAMAGES, LOST PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY DAMAGES FOR ANY BREACH OF THE TERMS OF THIS AGREEMENT OR FOR LOST OR CORRUPTED DATA ARISING FROM ANY CLAIM OR ACTION HEREUNDER, BASED ON CONTRACT, TORT OR OTHER LEGAL THEORY AND WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. HAIVISION SHALL NOT BE LIABLE FOR DAMAGES FOR ANY CAUSE WHATSOEVER IN AN AMOUNT IN EXCESS OF THE FEE PAID TO HAIVISION BY YOU FOR THE RELEVANT PRODUCT.

5. INDEMNIFICATION

5.1 Indemnification by Haivision.

(a) Haivision shall indemnify and hold You harmless against any and all actions, claims, losses, damages, liabilities, awards, costs and expenses (including reasonable attorneys' fees) ("Claims") arising out of i) any accusation or purported violation of any third person's US and copyright, trademark, patent rights or trade secrets, proprietary information on account of Your use of the Licensed Software when used in accordance with the terms of this Agreement, or (ii) relating to or arising out of any negligence or wilful misconduct on the part of Haivision or any breach by Haivision of the terms of this Agreement or any Maintenance and Support Agreement, or applicable law. You shall promptly notify Haivision in writing of any such Claim and promptly tender the control of the defense and settlement of any such Claim to Haivision. Haivision shall thereafter undertake the defense of any such Claim using counsel of its choice. You shall cooperate with Haivision, in defending or settling such Claim at the expense of Haivision; provided that Haivision shall not settle any Claim against You which would require the payment of money by You without the prior written consent of You, which consent shall not be unreasonably withheld. You shall have the right to consult and provide input into the defense with counsel of its choice at its own expense. Haivision shall not reimburse You for any expenses incurred by You without the prior written approval of Haivision, which approval shall not be unreasonably withheld.

(b) If any Licensed Software is, or in the opinion of Haivision may become, the subject of any Claim for infringement, then Haivision may, or if it is adjudicatively determined that any of the Licensed Software infringes in the manner described above (except to the extent that any translation, modification, addition or deletion or combination by You is the sole source of such Claim), then Haivision shall, at its option, either (i) procure for You the right to continue use of the Licensed Software for the term hereof, (ii) replace or modify the Licensed Software with other suitable and reasonably equivalent products so that the Licensed Software becomes non-infringing, or (iii) terminate this Agreement and refund to You a portion of the fee paid for the relevant Product.

(c) Haivision shall have no liability for: (i) the use of other than the then current release of the Licensed Software; (ii) the use of the Licensed Software other than as set forth in its accompanying documentation and as permitted herein; (iii) the modification of any of the Licensed Software by any party other than Haivision; or (iv) any infringement arising from the use of any Licensed Software by You after Haivision has issued a written notice to You requiring You to cease using such Licensed Software when Haivision exercises its option to terminate the License pursuant to Section 3.2 (collectively, "Exclusions"). SECTION 5.1 STATES HAIVISION'S ENTIRE OBLIGATION WITH RESPECT TO ANY CLAIM REGARDING THE INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

5.2 Indemnification by You. You shall indemnify and hold Haivision harmless against any and all Claims directly or indirectly arising out of, or in any manner whatsoever associated or connected with Your performance, purported performance or non-performance of its rights and obligations under this Agreement, and against any and all Claims incurred by or on behalf of any of the foregoing in the investigation or defense of any and all such Claims.

6. OTHER PROVISIONS

6.1 Export and Other Restrictions. This Agreement, and all Your rights and Your obligations under this Agreement, are subject to all applicable Canadian and U.S. Government laws and regulations relating to exports including, but not limited to, the U.S. Department of Commerce Export Administration Regulations and all administrative acts of the U.S. Government thereunder. In the event the Licensed Software or the Hardware is exported from the United States or re-exported from a foreign destination, You shall ensure that the distribution and export/re-export of the Licensed Software or the Hardware is in compliance with all laws, regulations, orders, or other restrictions of the U.S. Export Administration Regulations. You agree that neither it nor any of its Affiliates will export/re-export any Licensed Software, Hardware, technical data, process, Products, or service, directly or indirectly, to any country for which the Canadian government or United States government (or any agency thereof) requires an export license, other governmental approval, or letter of assurance, without first obtaining such license, approval or letter.

6.2 Publicity. Neither party shall make or authorize or permit any other person to make any announcement or other like statement concerning this Agreement or the subject matter, terms or conditions hereof, without the other party's prior written consent.

6.3 Transfer and Assignment. Haivision may assign, sublicense, or transfer this Agreement and/or any or all of its rights or obligations hereunder. You may not assign, transfer or delegate any of its rights or obligations hereunder (whether by operation of law or otherwise) without the prior written consent of Haivision. Any unauthorized assignment, transfer or delegation by You shall be null and void. No other Person shall have or acquire any right under or by virtue of this Agreement.

6.4 Waiver and Amendment. No modification, amendment or waiver of any provision of this Agreement shall be effective. No failure or delay by either party in exercising any right, power or remedy under this Agreement, except as specifically provided herein, shall operate as a waiver of any such right, power or remedy. Without limiting the foregoing, any terms and conditions of the Entitlement or similar materials submitted by either party to the other shall be of no force or effect.

6.5 Enforcement by Third Party. For any Licensed Software licensed by Haivision from other suppliers, the applicable supplier is a third party beneficiary of this Agreement with the right to enforce directly the obligations set forth in this Agreement against You.

6.6 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the Province of Québec, Canada and the Laws of Canada applicable therein (excluding any conflict of laws rule or principle, foreign or domestic).

6.7 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, such provision shall be changed and interpreted so as to best accomplish the objectives of the original provision to the fullest extent allowed by law and the remaining provisions of this Agreement shall remain in full force and effect.

6.8 Force Majeure. Neither party shall be liable to the other party for any failure or delay in performance to the extent that such delay or failure is caused by fire, flood, explosion, war, terrorism, embargo, government requirement, labor problems, export controls, failure of utilities, civil or military authority, act of God, act or omission of carriers or other similar causes beyond its control. If any such event of force majeure occurs, the party delayed or unable to perform shall give immediate notice to the other party, and the party affected by the other's delay or inability to perform may elect, at its sole discretion, to terminate this Agreement or resume performance once the condition ceases, with an option in the affected party to extend the period of this Agreement up to the length of time the condition endured. Unless written notice is given within 30 calendar days after the affected party is notified of the condition, the latter option shall be deemed selected. During an event of force majeure, the affected party shall exercise reasonable effort to mitigate the effect of the event of force majeure.

If you have questions, please contact Haivision Network Video, 4445 Garand, Montréal, Québec, H4R 2H9 Canada.