HAIVISION

Haivision Gateway 3.6
User's Guide

HVS-ID-UG-MGW-3.6

Edition Notice

About Haivision

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

Trademarks

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

Disclaimer

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

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

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

Contents

About This Document

Conventions

The following conventions are used to help clarify the content.

Typographic Conventions and Elements

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

Action Alerts

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

> ✓ **Tip**
>
> Indicates highlights, suggestions, or helpful hints.

> ⚠ **Note**
>
> Indicates a note containing special instructions or information that may apply only in special cases.

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

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

> ⚠️ **Warning**
>
> Indicates a potentially hazardous situation that may result in physical harm to the user.

Obtaining Documentation

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

Getting Service Support

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

Touring the Interface

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

> ⚠ **Note**
>
> To install a VM or cloud server or connect a hardware appliance, please refer to the appropriate **Quick Start Guide**.

Topics Discussed

- **Product Editions**
- **Features**
- **Basic Layout and Elements**
    - **Persistent Screen Elements**
    - **Variable Screen Elements**
- **Interface Screens**
    - **Sign In Screen**
    - **Route List Screen**
    - **Administration Screens**
    - **Preferences/About Screen**

Product Editions

With the version 3.2 release, Haivision Media Gateway is now available for broadcast workflows as Haivision SRT Gateway. Haivision SRT Gateway gives you access to expanded functionality with SRT and RTP streams, while Haivision Media Gateway is geared toward HMP enterprise workflows, as explained in the following diagram and sections.
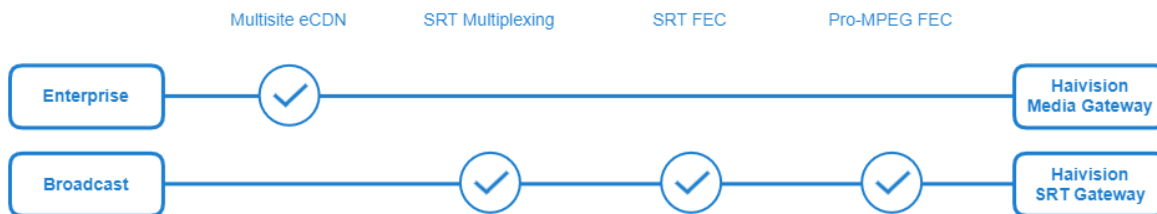
Haivision Media Gateway

The Haivision Media Gateway enables low latency live video streaming and conversion between protocols including RTP, RTMP, RTSP, HLS, TS over UDP, and the open-source SRT protocol for bridging between networks and distributing streams across multiple destinations. The Haivision Media Gateway helps

enterprise customers leverage eCDN functionality for Haivision Media Platform workflows including all-hands meetings and IPTV delivery.

Haivision SRT Gateway

The Haivision SRT Gateway enables low latency live video streaming and conversion between protocols including RTP, RTP-FEC, RTMP, RTSP, HLS, TS over UDP, and the open-source SRT protocol for bridging between networks and distributing streams across multiple destinations. The Haivision SRT Gateway helps broadcasters with live production contribution, backhaul, remote monitoring, bi-directional live interviews, and video distribution.

> ⚠️ **Note**
>
> Licenses are available to convert your Haivision Media Gateway to Haivision SRT Gateway. Contact your Haivision representative for more details.

Features

Haivision's Media Gateway and SRT Gateway are networking infrastructure products for configuring, monitoring, and managing streaming routes between encoding and decoding devices. They are 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.

This section summarizes product features of Haivision Media Gateway (HMG) and Haivision SRT Gateway (HSG).

Transport High Quality Video Over Any Network

Haivision Media Gateway and Haivision SRT Gateway support Haivision's open-source SRT (Secure Reliable Transport) protocol - a technology that optimizes live video distribution across unpredictable networks, like the Internet, by assuring quality-of-service when faced with packet loss, congestion, jitter, latency, and fluctuating bandwidth. Leveraging SRT, the Haivision Media Gateway/SRT Gateway is ideal for transporting high-quality, low latency, and secure live video across public and private networks, and offers significant operational flexibility and cost savings compared to satellite or custom network infrastructures.

Network Bridging

Haivision Media Gateway and SRT Gateway help take video streams from one network environment to another. Whether bridging between LANs, MPLS, satellite IP, public internet, or any combination of these networks, the Haivision Media Gateway/SRT Gateway is the perfect element thanks to its advanced network interface configuration, native SRT protocol support, and friendly firewall traversal. In addition, it is codec agnostic and provides support for any standard MPEG stream – future proofing every solution.

Video Ecosystem Compatibility

Haivision Media Gateway and SRT Gateway convert streams between SRT, Transport Stream over UDP (unicast and multicast), and can also input RTSP and RTMP and output HLS. As a component of an end-to-end video workflow, HMG/HSG supports stream interoperability directly with Haivision's Makito X family of encoders and decoders, Haivision's transcoders, the high performance InStream Mobile player for iPhone and Android, and any standard third-party UDP streams, giving the flexibility to extend virtually any video workflow over any network.

> ⚠️ **Note**
>
> The re-distribution of HLS streams originating from non-Haivision sources is not supported at this time.

Firewall Friendliness

IP firewalls block external access to a network and prevent video streams from being delivered from one location to another. A Haivision Media Gateway/SRT Gateway can be configured anywhere so that behind-the-firewall devices can reach streams without breaching network security policies and minimizing the need for IT intervention.

Encryption

End-to-end stream encryption (AES 128/256) is available to prevent unauthorized viewing, recording, and redistribution of private content.

Multi-site Live Streaming Support

Seamlessly integrated with Haivision's enterprise video platform, the Haivision Media Gateway creates a secure enterprise content delivery network (eCDN) extending internal broadcasts, all hands meetings, and on-demand video libraries to remote locations and scales video delivery to thousands of employees.

Basic Layout and Elements

The Web interface groups device management into the following main screens: Route List (home) and Administration. These screens use a consistent layout with common screen elements to simplify your experience.
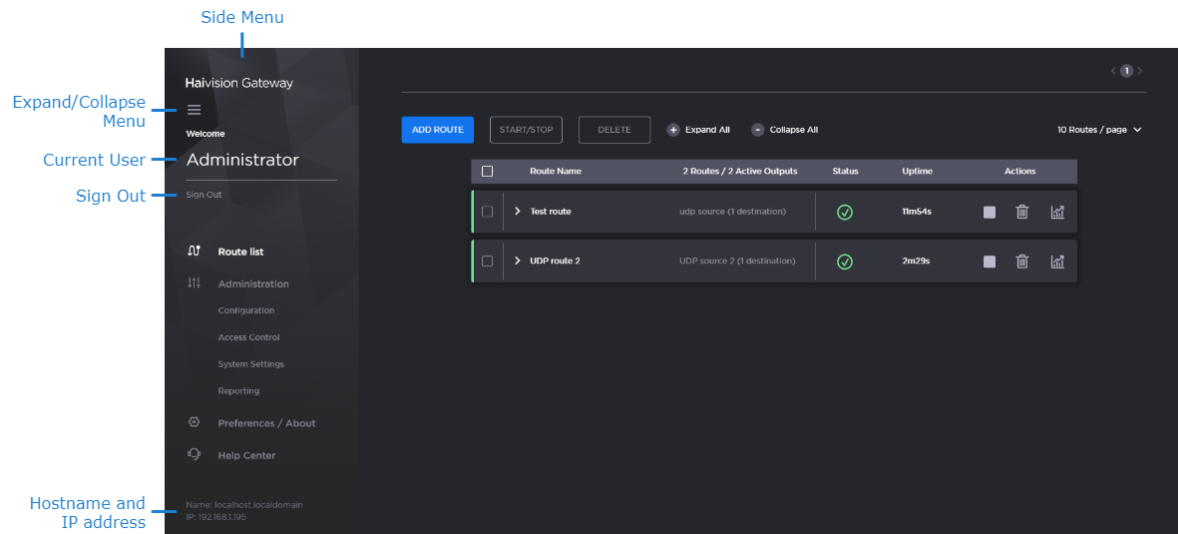
Persistent Screen Elements

The following elements are constant and available from any screen.

Expand/Collapse Menu Button

Clicking the ☰ icon, expands and collapses the menu toolbar.

Current User

Identifies the user who is currently signed into the system.

Sign Out

Clicking Sign Out exits the system and returns you to the Sign In screen.

Side Menu

The available items in the side menu depends on the account you are signed into. The side menu provides access to:

- Route List 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.
- Preferences/About screen — Opens a screen to configure user preferences including user interface brightness and contrast control and browser cache reset. Also displays the version number, build number, and copyright statement.

> ✅ **Tip**
>
> When requesting assistance, provide the build number to the support representative.

- Help Center button — Opens the Haivision InfoCenter website to view the Haivision Media Gateway/SRT Gateway documentation.

> ⚠️ **Note**
>
> If no external internet connection is available, a local documentation file is opened in your web browser. Always refer to the Haivision InfoCenter for the latest documentation.

Hostname and IP Address

The bottom left of the side menu shows the Gateway's hostname and IP address to help you identify the device you are currently monitoring. You may change the hostname in the **Administration** > **System Settings** > **Network** page. See **Configuring the Network** for details.

Variable Screen Elements

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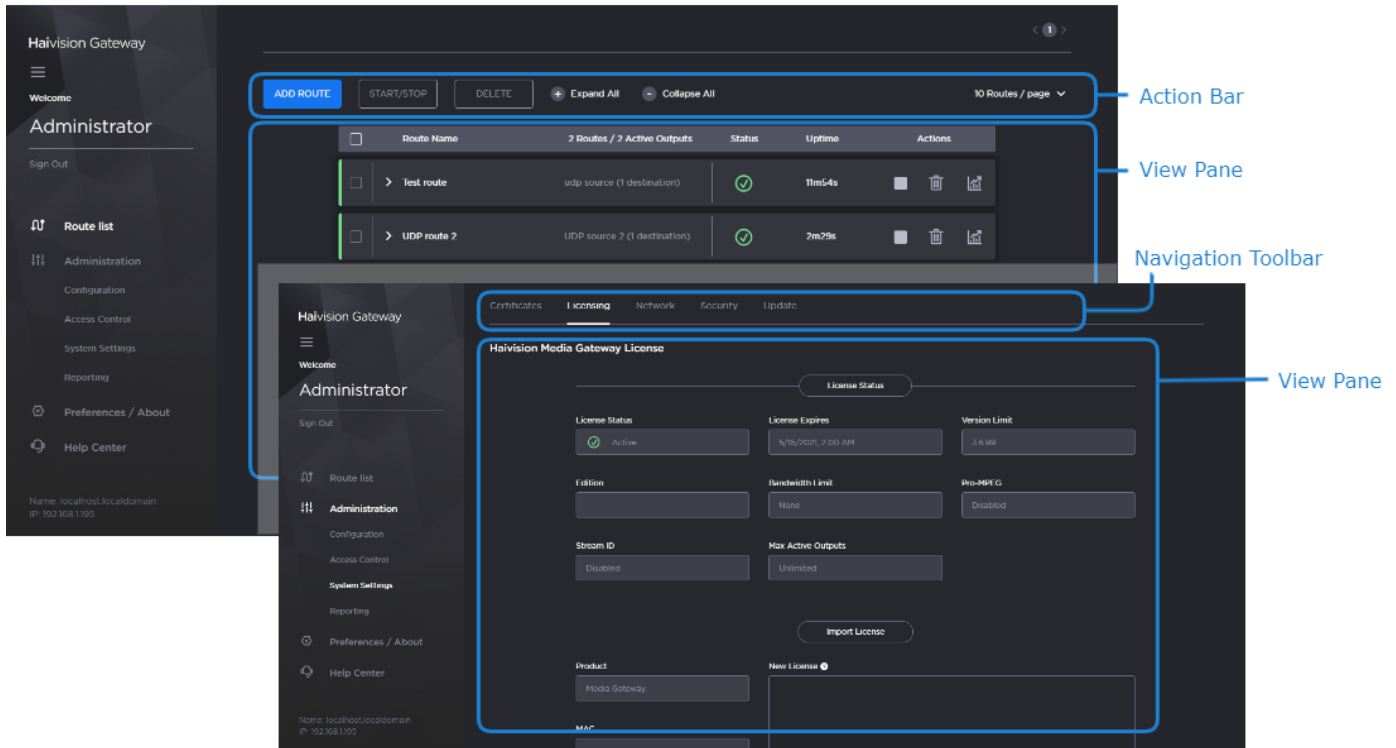
Action Bar

On the Route List screen, the action bar provides buttons for managing and displaying routes available in the view pane.

Navigation Toolbar

Selects the category of the currently selected administration group shown in the sidebar.

View Pane

The view pane displays the appropriate items, fields, or status information for the currently selected screen.

Interface Screens

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

Sign In Screen

When you first browse to the web interface, a Sign In screen appears prompting you to sign into the system.
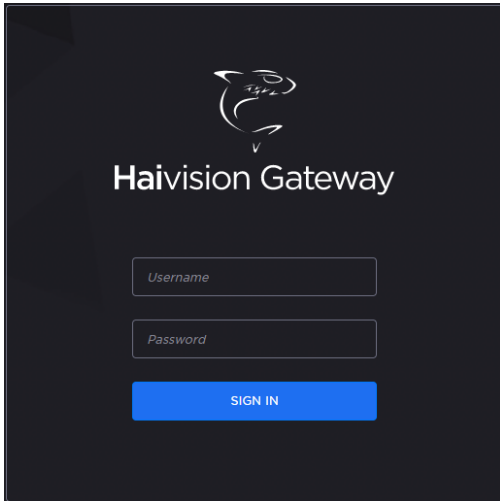
After you sign in, the Route List screen appears.

Related Topics
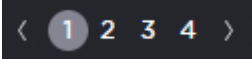
- **Signing into the Web Interface**

Route List Screen

The Route List screen gives you an overview of the currently defined routes. You can expand/collapse the routes to list more information regarding their source and destinations.

Various elements appear as shown in the following figure, and they are each described below.

Element	Description
Add Route button	Click to add a new route. See Creating a Route.
Start/Stop button	Select the checkboxes next to the routes you wish to start/stop, and click the **Start/Stop** button. See Starting, Stopping, and Deleting a Route.
Delete button	Select the checkboxes next to the routes you wish to delete, and click the **Delete** button. See Starting, Stopping, and Deleting a Route.
Expand All/Collapse All buttons	Expands/Collapses the source and destination route details.
Pagination option	Select how many routes to show per page.
Page buttons	If the number of defined routes is greater than the pagination option, then page buttons are available to go to other pages. For example: ‹ 1 2 3 4 ›
Collapsed/Expanded Route	Clicking the ❯ / ❯ icons next to a route collapses or expands the route. • When collapsed (❯ icon appears), the route listing shows the name of the route, the source name and number of destinations, the route status icon, the current uptime if the route is not stopped, and action buttons to start/stop, delete, and view the statistics of a route. Clicking the elsewhere in the route opens the Edit Route screen. • When expanded (❯ icon appears), the route listing also shows the source and destination stream details including names, protocol, type, individual status icons, address and action buttons to start/stop each destination. Clicking the source stream opens the Edit Route screen, and clicking a destination stream opens its Edit Destination dialog. See the following for a desciption of the status icons.

Status Icons

Hovering over the status icon shows more details regarding the status.

Icon	Description
⊘	Active with data flow.
△	Connection in progess.
⊖	Inactive/Idle.
☀	Starting or updating route.
☀	Stopping route.

Administration Screens

If logged in as an administrator, the Administration screens allows you to configure various options for your Haivision Media Gateway/SRT Gateway. The options on each of the four administration screens are grouped into categories listed in a toolbar at the top of the screen. The currently selected category is

indicated as bold and underlined. The view pane displays the appropriate fields or items for your chosen category. Likewise, selections made in the view pane may also alter the available fields or options in the view pane. For example:
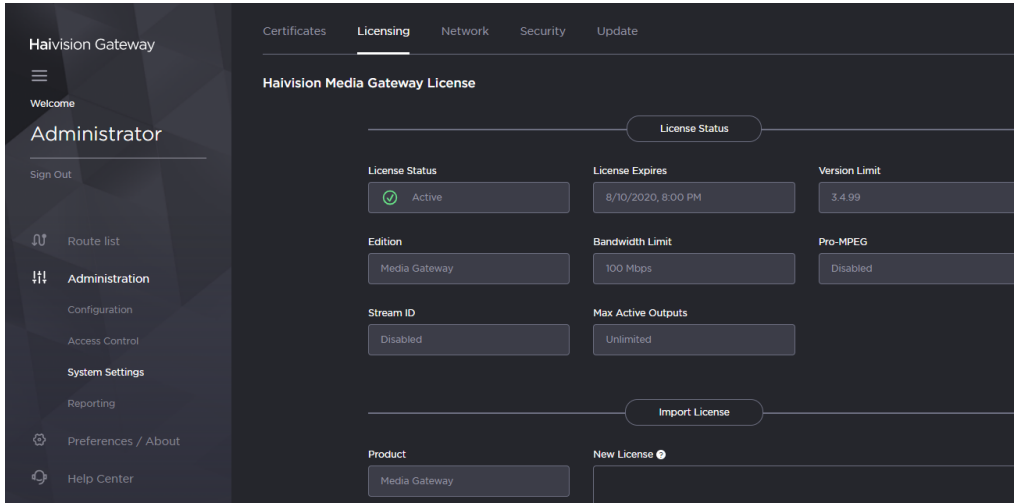
To navigate to the Administration screens, click one of the sections under **Administration** in the side menu. The available sections and subsequent screens are:

Administration Sections	Available Screens
Configuration	**Media Platform** — Provides the status and settings pane for pairing the Media Gateway with a Haivision Media Platform server. **Presets** — Allows you to export the current configuration as a preset file and import a preset file and apply it to the device.
Access Control	**Accounts** — Identifies the current roles (administrator, operator, and observer) on the system and the members for each. Allows you to change the user passwords.
System Settings	**Certificates** — Allows you to install an TLS security certificate. **Licensing** — Allows you to add/update licenses and view their limits and status. **Network** — Provides access to the network configuration settings, as well as information on the interfaces. **Security** — Allows you to enable FIPS compliance, high-security environment, and an advisory banner. **Update** — Identifies the currently installed bundle and allows you to update to a new version of software.
Reporting	**Report** — Offers access to a number of different logs providing system, application, and diagnostic messages. **System Activity** — Provides quick statistics on the system (bandwidth and CPU/memory usage), hardware information, and disk space statistics. **Detailed Info** — Provides detailed charts of the system statistics (bandwidth and CPU/memory usage).

Preferences/About Screen

The Preferences/About screen allows you to:

- Customize the brightness and contrast of the web interface.
- Change the color scheme of the interface: light or dark.
- View the current product edition, version, and build of your software.

To adjust brightness and contrast of the web interface:

1. In the side menu click **Preferences/About**.
2. Under the Preferences section, adjust the sliders to the desired brightness and contrast settings.
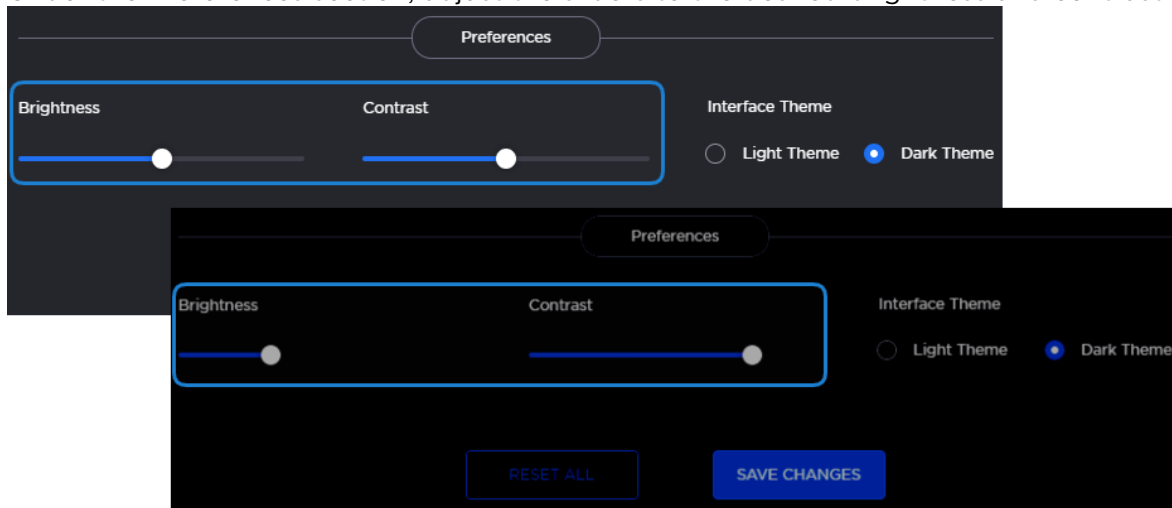
3. Click the **Save Changes** button to save the settings, or click the **Reset All** button to restore the default brightness and contrast.

To change the color theme of the interface:

1. In the side menu click **Preferences/About**.
2. Under the Preferences section, select either Light Theme or Dark Theme.
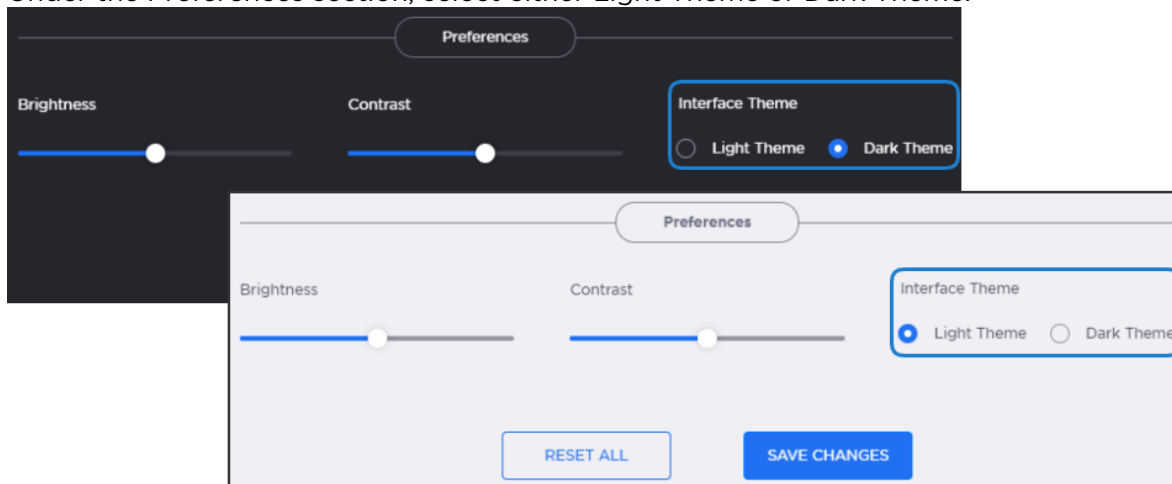
3. Click the **Save Changes** button to save your change.

To view the current version and build of your software:

1. In the side menu click **Preferences/About**.
2. Under the **About** section, the product edition, version number, and build number is shown.

Haivision Media Gateway

Version 3.4.0   Build 356

Copyright © 2012-2020 Haivision Network Video Inc. All Rights Reserved.

Getting Started

The following content explains how to access and sign into the web interface.

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

Topics Discussed

- **Signing into the Web Interface**
  - **TLS Encryption**
- **Signing Out of the Web Interface**
- **Changing Passwords**
- **Setting Up a Test Route**
  - **Setting Up a Source Stream**
  - **Setting Up a Destination**
  - **Creating a Route**

Signing into the Web Interface

> ⚠ **Note**
>
> - Internet Explorer is no longer supported. We recommend using Microsoft Edge or Google Chrome.
> - To sign into web interface, ensure that you have enabled cookies in your browser.

To access the web interface:

1. Open a web browser and enter the URL or IP address of the Media Gateway/SRT Gateway server in the address bar. For instance:

   `http://<ipaddress>` or `http://<systemurl>` where

   - `<ipaddress>` is the IP address of the system where server is installed. For example, http://10.69.12.152 .
   - `<systemurl>` is the system's URL, such as http://gateway.haivision.com.

   See the appropriate Quick Start Guide for details on obtaining the IP address of the server.
2. When the browser accesses the web interface, 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. (Responses vary depending upon the browser used.) See **TLS Encryption** for more details.
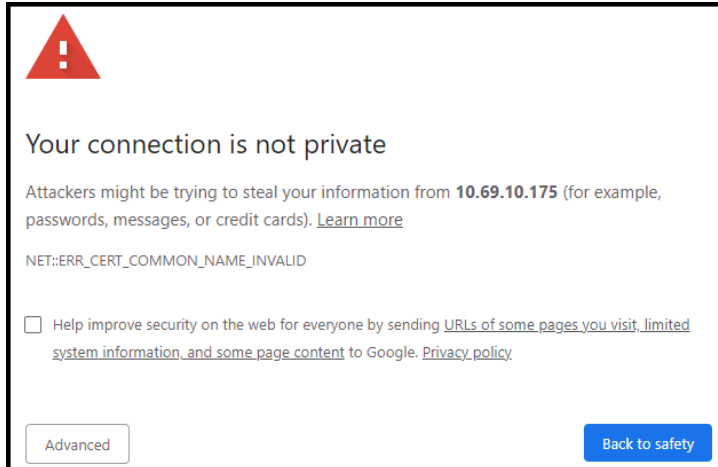
> ⚠️ **Important**
>
> Before proceeding or adding an exception for the site, check with your administrator on the correct response.

3. At the Sign In screen, enter your username and password. See the *Important Notice* document for the default credentials.
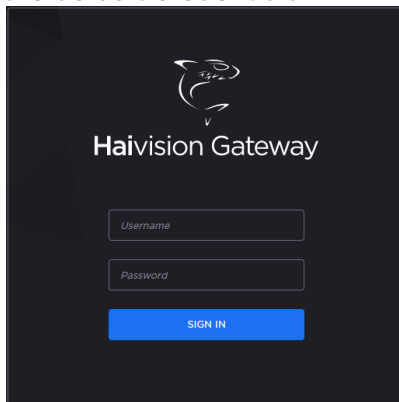
4. Click the **Sign In** button. The Web interface opens to the Route List screen.

Related Topics

- **Sign In Screen**
- **Signing Out of the Web Interface**
- **TLS Encryption**
- **Changing an Account's Password**

TLS Encryption

The Media Gateway/SRT Gateway web interface is encrypted to provide secure interactions with your devices. When you access the web interface, you are automatically redirected to use HTTPS on port 443. As a result, your web browser requests the security certificate to confirm that the site is trusted. Media Gateway/SRT Gateway ships with a self-signed TLS 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.

> ⚠️ **Note**
>
> Recent OS updates (particularly macOS 10.15 and iOS 13, see **https://support.apple.com/en-us/ HT210176**) block access to websites with TLS certificates that have a validity window of more than 825 days. Previous versions of Haivision Media Gateway ship with a self-signed certificate with a 10-year expiration, while Haivision Media Gateway/SRT Gateway version 3.2+ ships with a self-signed certificate with a 2-year expiration. Therefore, new installs are not affected by this issue. However, if you have upgraded from a previous version to version 3.2 or later, you must generate a new certificate to allow access. From a computer that can access the server, use an administrator account to regenerate a new self-signed certificate. See **Generating a New Self-Signed Certificate** for details on how to do this.

Supplying the Media Gateway/SRT Gateway with an TLS security certificate eliminates the security warning, provides a means for users to verify a website, and ensures that the connection is secure. See **Certificates** for more details.

Signing Out of the Web Interface

When signed into the Web interface, click the **Sign Out** action link at the left side of any screen to sign out.
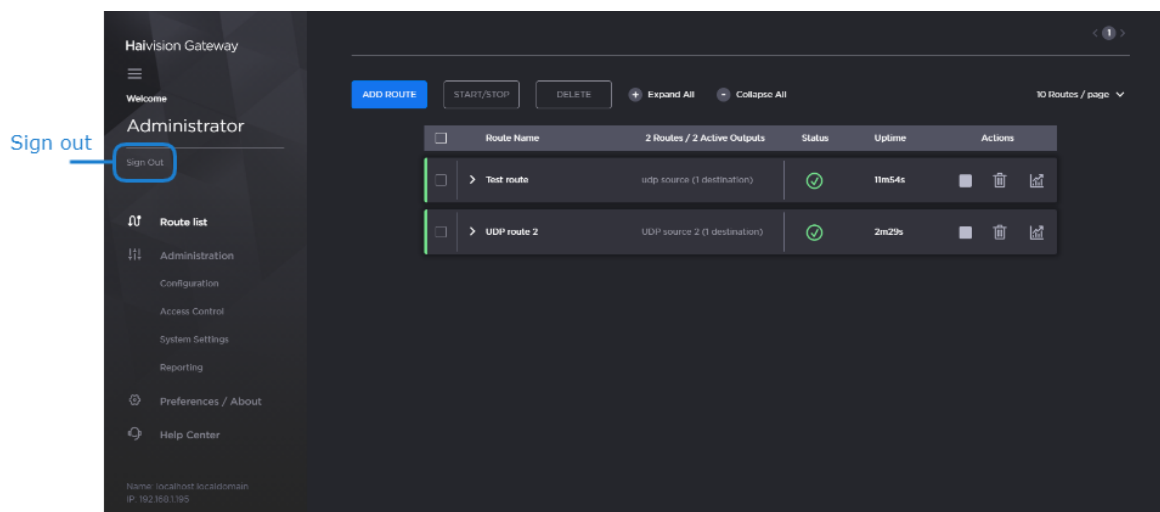
> ⚠️ **Note**
>
> If there is no activity over a period of ~2 minutes, the system automatically signs you out of the session.

Related Topics

- **Persistent Screen Elements**
- **Signing into the Web Interface**

Changing Passwords

> ⚠️ **Important**
>
> - For security purposes, change the default password for each of the available accounts. Information regarding user/password credentials should be safe-guarded. See Changing an Account's Password for details of changing passwords.
> - Factory-set passwords are provided in the *Important Notice* document.

Setting Up a Test Route

Media Gateway/SRT Gateway allows you to create and manage "routes", which consist of a *source* and a *destination* (along with other parameters, such as the incoming and outgoing transport protocols). You can verify that your server is operating normally by setting up a test route. To do this, you need to:

1. Set up a **source** (e.g., configure a video stream output on a Makito X4 Encoder).
2. Set up a **destination** (e.g., configure a Makito X4 Decoder to play back the source stream).
3. Create a **route** on the Media Gateway/SRT Gateway server (receive the stream from the source and then relay it to the destination).

> ⚠️ **Note**
>
> To get you started, the following instructions show you how to set up simple unicast stream to and from the Media Gateway/SRT Gateway. For information on how to set up other stream types and combinations, including multicast and SRT, please refer to Creating a Route.

Setting Up a Source Stream

The following example of setting up a test stream requires that you have a Makito X4 Encoder with an active video input. You need to configure one of the Makito X4 internal encoders based on your video source, and then configure an output stream for that encoder.

> ✅ **Tip**
>
> As you set up the test stream, you may wish to refer to the *Makito X4 User's Guide*, available from the Haivision InfoCenter.

> ⚠️ **Important**
>
> The IP address of your computer must be in the same subnet.

1. If you have not already done so, power up the Makito X4 Encoder.
2. Open a Web browser to the IP Address for the Makito X4 and log in.
   The Web interface opens to the Outputs List View.
3. Click **Video Encoders** in the sidebar to configure the video encoders.
4. On the Video Encoders List View, click a link in the table to select an encoder.
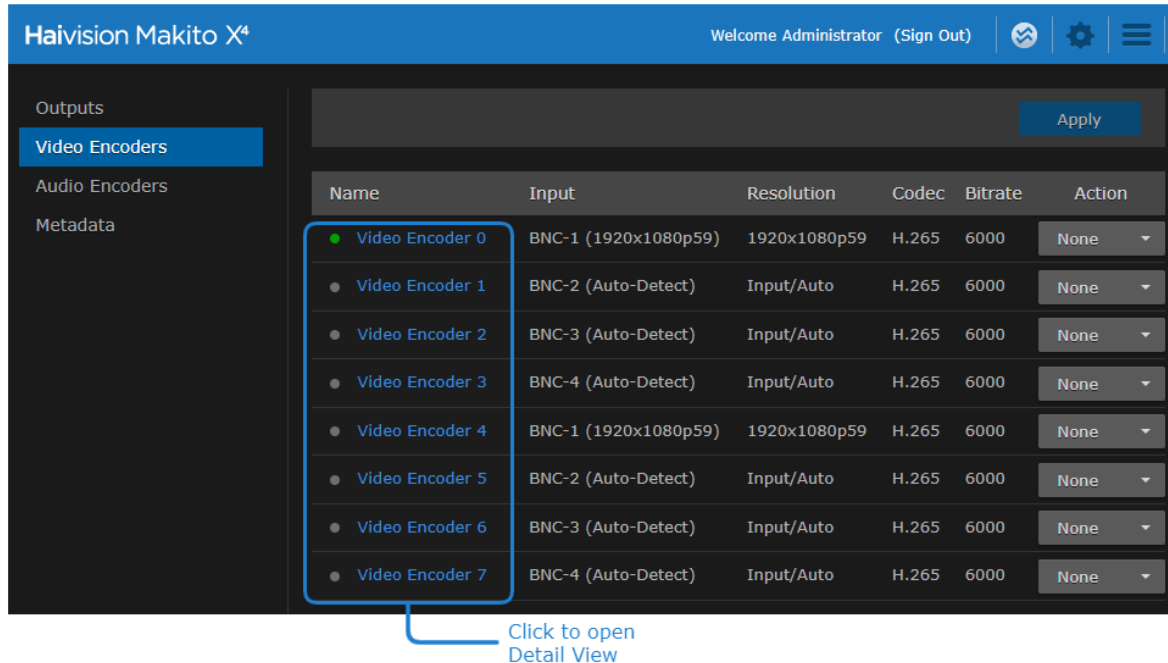
The Video Encoder Detail View opens, displaying the settings for the selected video encoder.

5. Select or enter the new values in the appropriate fields.
6. Click the **Start** button, and then click **Apply**.
7. To set up streaming, click **Outputs** in the sidebar.
8. To add an output stream, click the ⊕ button.
9. On the New Stream page, type a Name for the stream and select the encoder you started in Step #6.
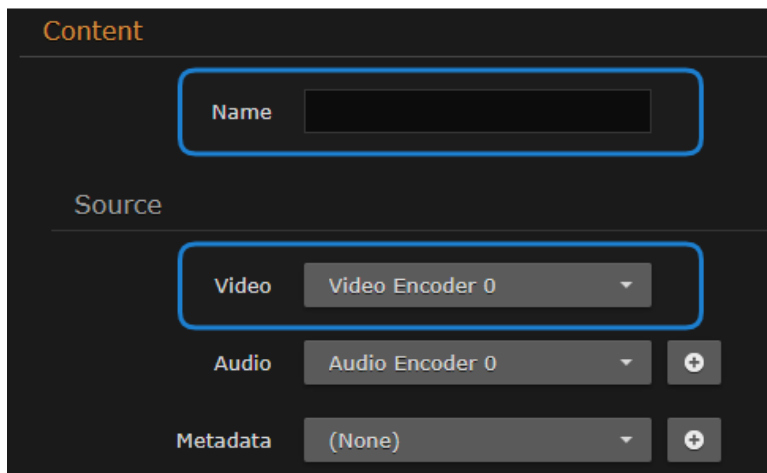
10. To set up streaming:
    • In the Broadcasting section, select TS over UDP for the Protocol.
    • In the Destination section, type in the IP Address of the Media Gateway/SRT Gateway, and specify a port number. (Remember this number for a future step in **Creating a Route**.)
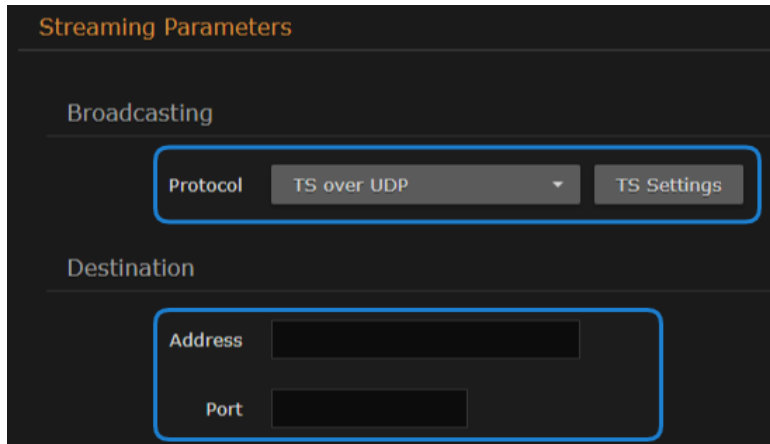
11. To apply your changes and start streaming, click the **Apply** button. The new stream appears in the list of output streams.

For more details, refer to the *Makito X4 User's Guide*.

Setting Up a Destination

To play back the test stream from the Media Gateway/SRT Gateway, you must configure a stream input on a Makito X4 Decoder.

> ✅ **Tip**
>
> As you configure the stream input, you may wish to refer to the *Makito X4 Decoder User's Guide*, available from the **Haivision InfoCenter**.

1. If you have not already done so, power up the Makito X4 Decoder.

> ⚠️ **Note**
>
> For the purpose of this test, you should connect a monitor to the SD1 output.

2. Open a Web browser to the IP Address for the Makito X4 Decoder and log in. The Web interface opens to the Streams List View, displaying the defined streams for the decoder.
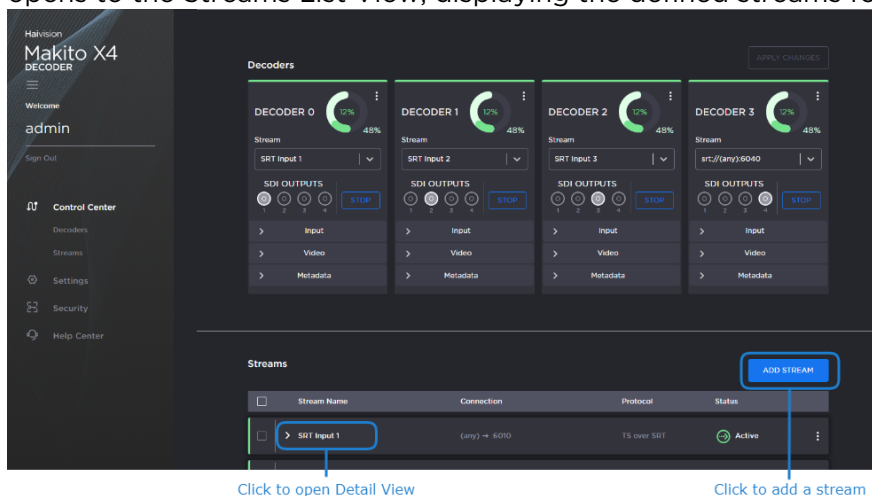
3. To add an incoming stream, click **+Add**.
4. On the New Stream page:

- In the Content section, type a Name for the stream and select **TS over UDP** for the Protocol.
- In the Source section, select Unicast and enter a port number that is different from the port number used in Step #10 in **Setting Up a Source Stream**. (Remember this number for a future step in **Creating a Route**.) Click **Create**.
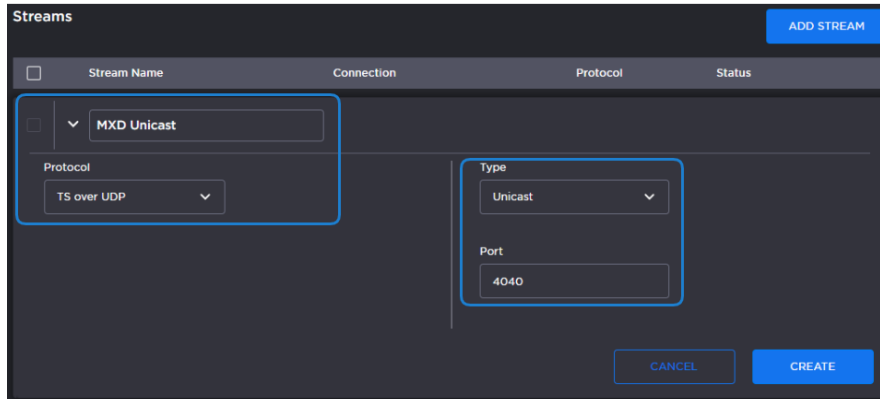
5. To configure the video output, select the decoder assigned to SDI Output 1, and choose the stream you created in Step #4.
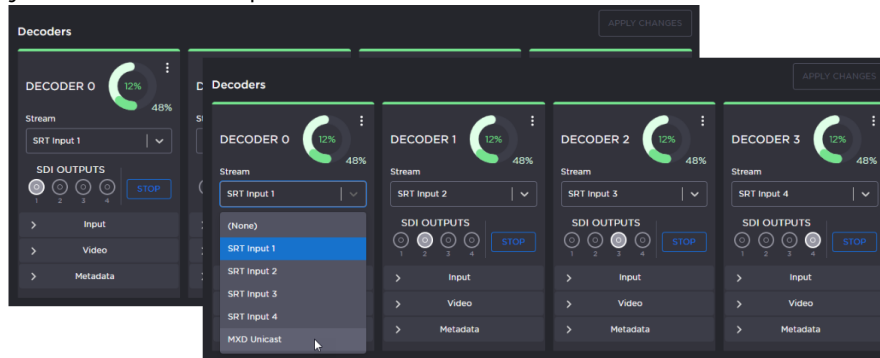
6. Click the **Apply Changes** button.

For more details, refer to the *Makito X4 Decoder User's Guide*.

Creating a Route

1. If you have not already done so, sign in to the Media Gateway/SRT Gateway Web interface.
2. On the Route List screen, click the **Add Route** button.
3. Supply a Route Name and check the **Start Once Created** checkbox so that the stream is started after you create it.
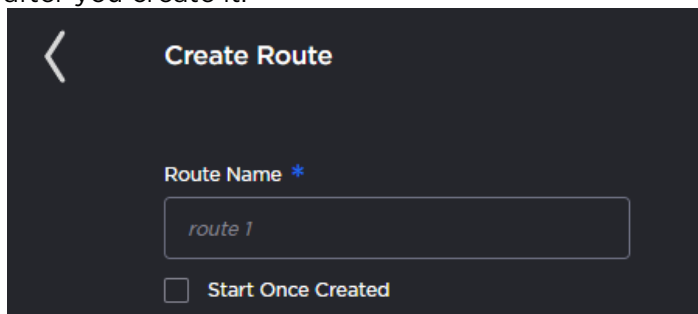
4. In the Source section, provide a Source Name, select **TS over UDP** for the Protocol (for this example), and enter the port number of the source Makito X4 Encoder (see Step #10 in **Setting Up**

a Source Stream).

5. Click the **Add Destination** button.
6. In the Add Destination dialog, provide a destination name, select **TS over UDP** for the protocol, and enter the IP Address and port number of the destination Makito X4 Decoder (see Step #4 in **Setting Up a Destination**).

7. When finished, click **Save**. The new route appears in the Destination list.
8. Click **Create**.
9. On the Route List screen, verify that after a few seconds the status indicator is green.

You should now see the video from the source Makito X4 Encoder relayed via Media Gateway/SRT Gateway to the monitor connected to the destination Makito X4 Decoder.

Working with Media Gateway and SRT Gateway

The following content discusses how to work with routes in detail on your Haivision Media Gateway/SRT Gateway server.

Topics Discussed

- Multi-site Live Workflow
  - Pairing the Gateways with Media Platform
  - Defining the Locations and Network Topology (Media Platform)
  - Source Forwarder
  - Source Receivers
- Multicast Workflow
  - Run-Through Example
  - Run-Through Example Recap
- Working with Routes
  - Creating a Route
  - Editing a Route
  - Starting, Stopping, and Deleting a Route
  - Viewing a Route's Statistics
- Working with Destinations
  - Editing the Destination
  - Starting, Stopping, and Deleting a Destination Node

Multi-site Live Workflow

Media Gateway works with Media Platform 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.

> ⚠ **Important**
>
> Haivision SRT Gateway is not meant for multi-site Haivision Media Platform workflows. The following sections apply to Haivision Media Gateway only.

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:

Locations corresponding to the networks served by each Media Gateway are defined in Haivision Media Platform (HMP)

Remote Location 1   **Main Location**   **Remote Location 2**

Haivision
Media Platform (HMP)

HMP is paired with each
Media Gateway

Pairing
request via
HTTPS
traverses
firewall, if
any

Haivision   Haivision   Haivision
Media Gateway 1   Media Gateway Main   Media Gateway 2

Video stream from encoder is
configured (in HMP) as source
to be sent to a Media Gateway

Source
(e.g., Makito X4 Encoder)

⚠ **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 and Network Topology (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**. For the workflow diagram shown in Pairing the Gateways with Media Platform and at the end of this section, three locations are defined: Main Location, Remote Location 1, and Remote Location 2.

After defining the locations in Media Platform, configure the network topology of these locations; that is, the ingoing and outgoing connections for each location. For the example shown below, the Main Location has an outgoing connection to Remote Location 1 and Remote Location 2. The resulting Topology page in Media Platform appears as follows:
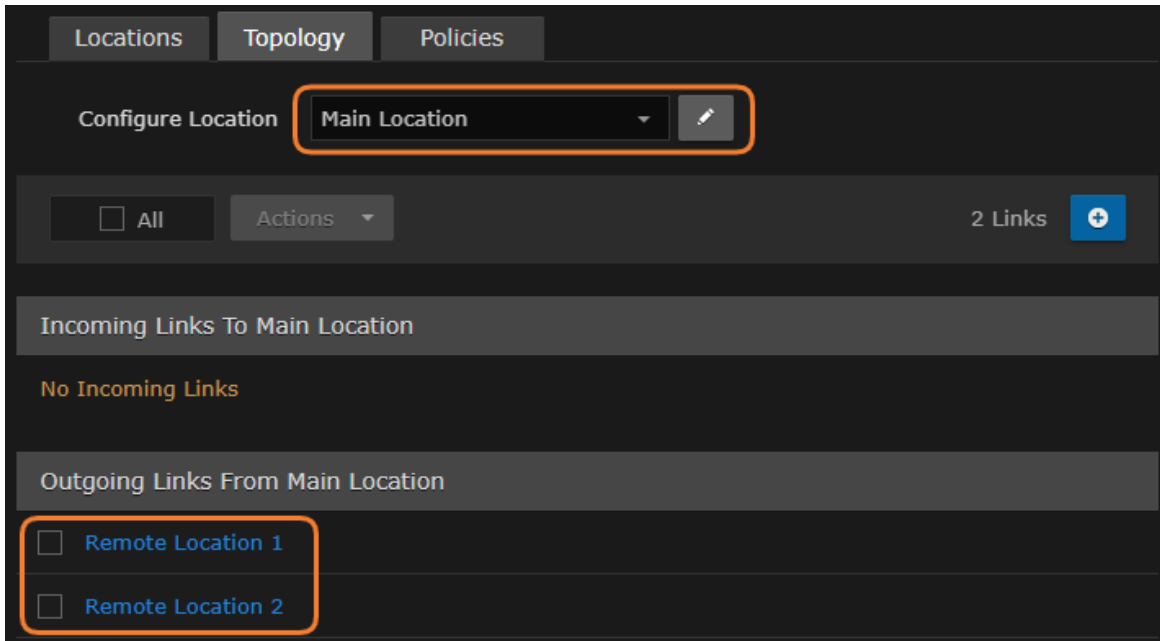
Based on these locations and network topology, Media Platform generates routing configurations for each of the locations. The respective Media Gateways poll the Media Platform at intervals of approximately 30 seconds, and download the routing configuration files.

> ⚠️ **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.
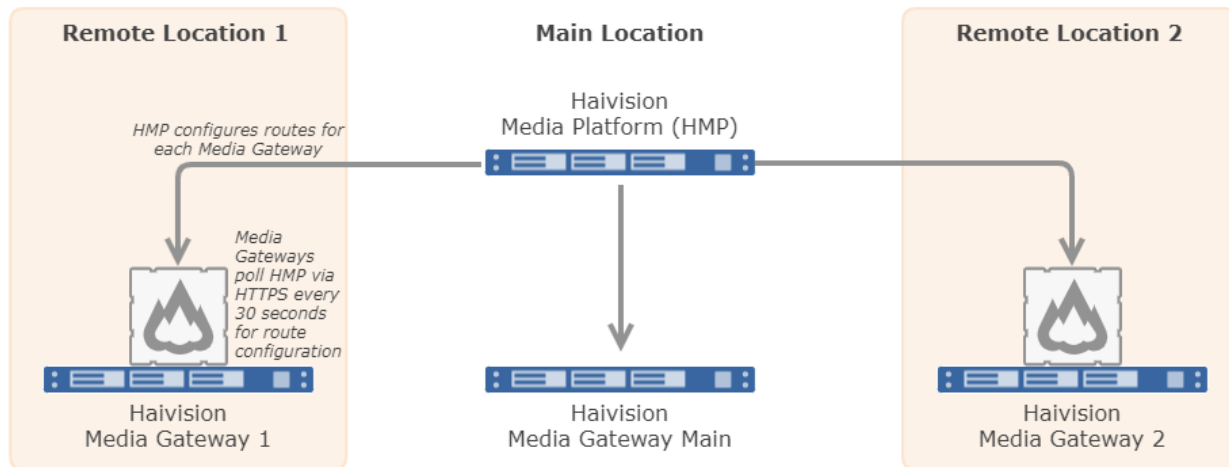
Source Forwarder

For the Media Gateway to which the video source is connected (the forwarder), Media Platform creates a route identified by a name with the following syntax: `[source_name] (HMP) [source_ID]`. A route with this name indicates that the Media Gateway is receiving traffic from a source (e.g., a Makito X4 Encoder)

and forwarding it to Media Platform. The `[source_name]` corresponds to the name of the live video source, and the `[source_ID]` corresponds to the ID of the live video source.

The number of destinations the route contains depends on the HMP locations and network topology settings. In the following sample screenshot, the route shows the Media Gateway (forwarder) propagates the source to four destinations: two corresponding to muxed and variant HLS streams for the local audience, one for forwarding the live video to a remote Media Gateways via SRT, and one SRT for Media Platform to access the video for recording:

> ⚠ **Note**
>
> The status of the HMP's SRT 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 to which the live video is being sent (the receiver), Media Platform creates a route identified by a name with the following syntax: `[source_name] (HMP) [source_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_name` corresponds to the name of the live video source, and the `source_ID` corresponds to the ID of the live video source.

> ⚠ **Note**
>
> An HMP session must have its Live button enabled for the route to be created at the receiver locations.

The number of destinations the route contains is dependent on the HMP location settings. In the following sample screenshot, the route shows the Media Gateway (receiver) propagates the source to three destinations, corresponding to SRT, a muxed HLS, and variant HLS streams 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.

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):
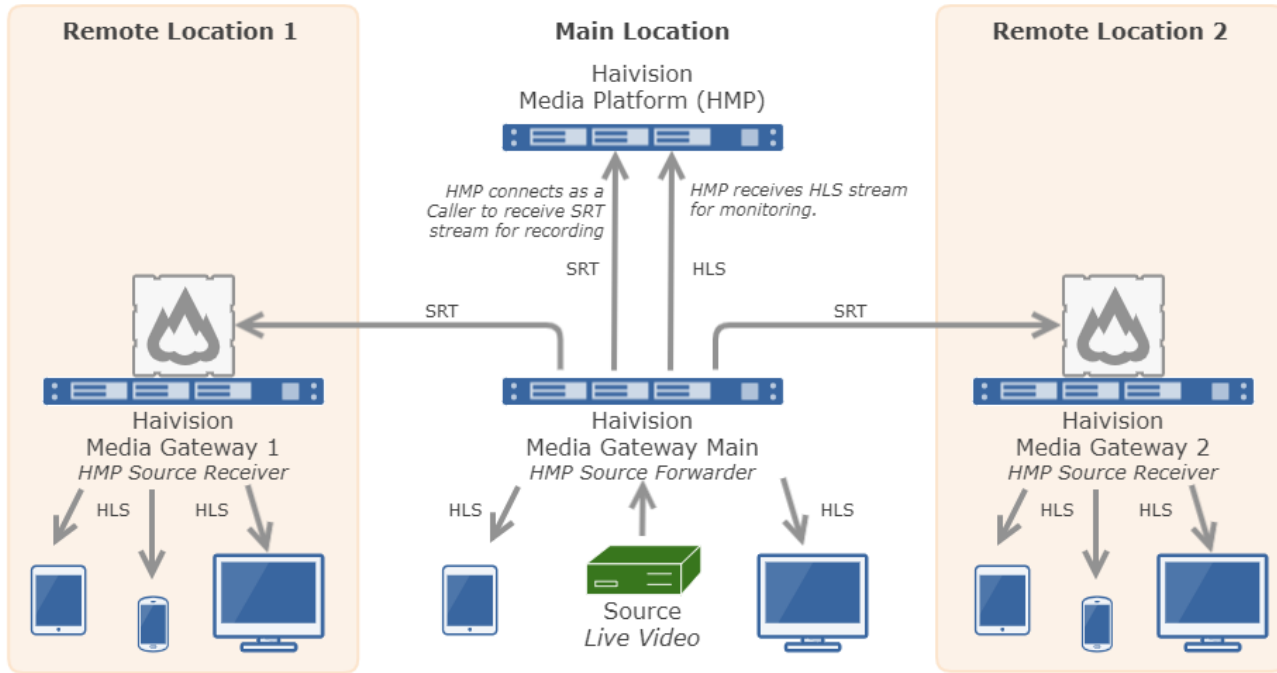
For more information, including complete instructions on how to configure a multi-site live session, please refer to the HMP Administrator's Guide.

Multicast Workflow

The following workflow steps you through an encoder sending an SRT stream to a hosted instance of Media Gateway/SRT Gateway on the cloud, which routes each destination segment. At the remote sites, a Media Gateway/SRT 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:
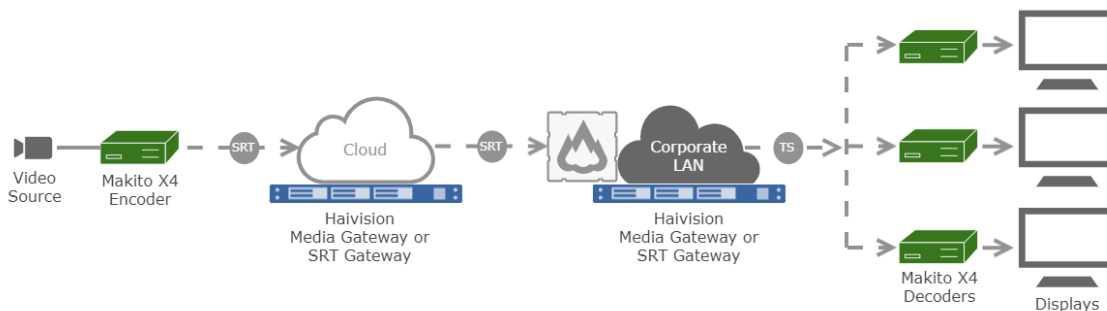
In the above diagram, the cloud-based Media Gateway/SRT Gateway (located on the Public Internet or as a Haivision Video Cloud (HVC) hosted option) is *optional* and only recommended for individuals who want to "own" the distribution or have concerns about low latency. A Media Gateway/SRT Gateway can also be hosted on the LAN to allow multi-sites distribution.

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

Run-Through Example

Before stepping through this example, the two Media Gateway/SRT Gateway installations must be available in the cloud and on your local area network.

Creating your Workspace (Optional)

> ✅ **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 X4 web interface of your source on one tab, the cloud Media Gateway/SRT Gateway on another, and so forth. This way, you can switch back and forth between them.

1. In your web browser, open a tab, enter the Makito X4 Encoder web interface URL, and log in when prompted.
2. Open another new tab, enter the cloud-based Media Gateway/SRT Gateway web interface URL, and sign in when prompted.
3. Open another new tab, enter the remote site's LAN-based Media Gateway/SRT Gateway web interface URL, and sign in when prompted.
4. Open another new tab, enter the Makito X4 Decoder web interface URL, and log in when prompted.
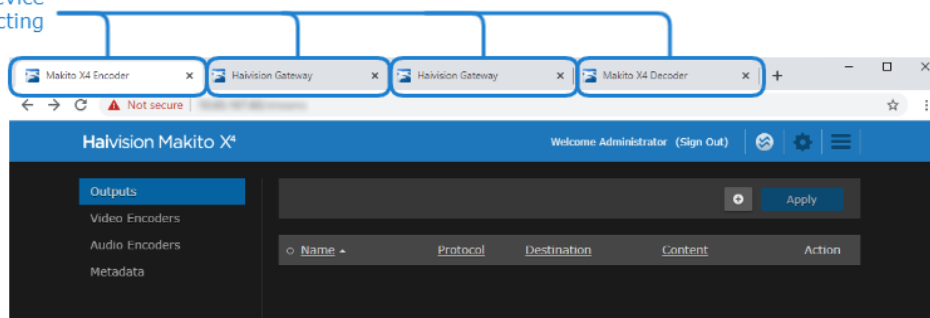
Establishing the Source

1. If you followed the steps in **Creating your Workspace (Optional)**, switch to the Makito X4 Encoder's browser tab. Else, enter the URL for the Makito X4 encoder web interface and log in when prompted.

2. On the Makito X4 Encoder's navigation sidebar, click **Outputs**.
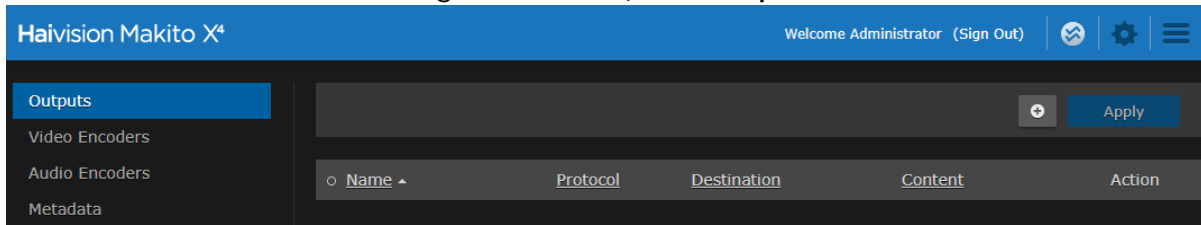
3. The view pane lists the available streams. For this example, we are going to add a stream that uses TS over SRT. Click the ⊕ button. If you have an existing SRT stream, you can modify it instead.

> ⚠ **Note**
>
> Refer to your **Makito X4 Encoder documentation** for more information on adding streams if you are new to this process.

4. When the New Stream screen opens:
    *   In the Content section, provide a (1) stream name. For (2) video, select an active video encoder.
    *   In the Streaming Parameters section, specify the (3) TS Over SRT protocol, the (4) mode as "Caller," enter the (5) address for the Media Gateway/SRT Gateway (in the Cloud) and a (6) destination port.
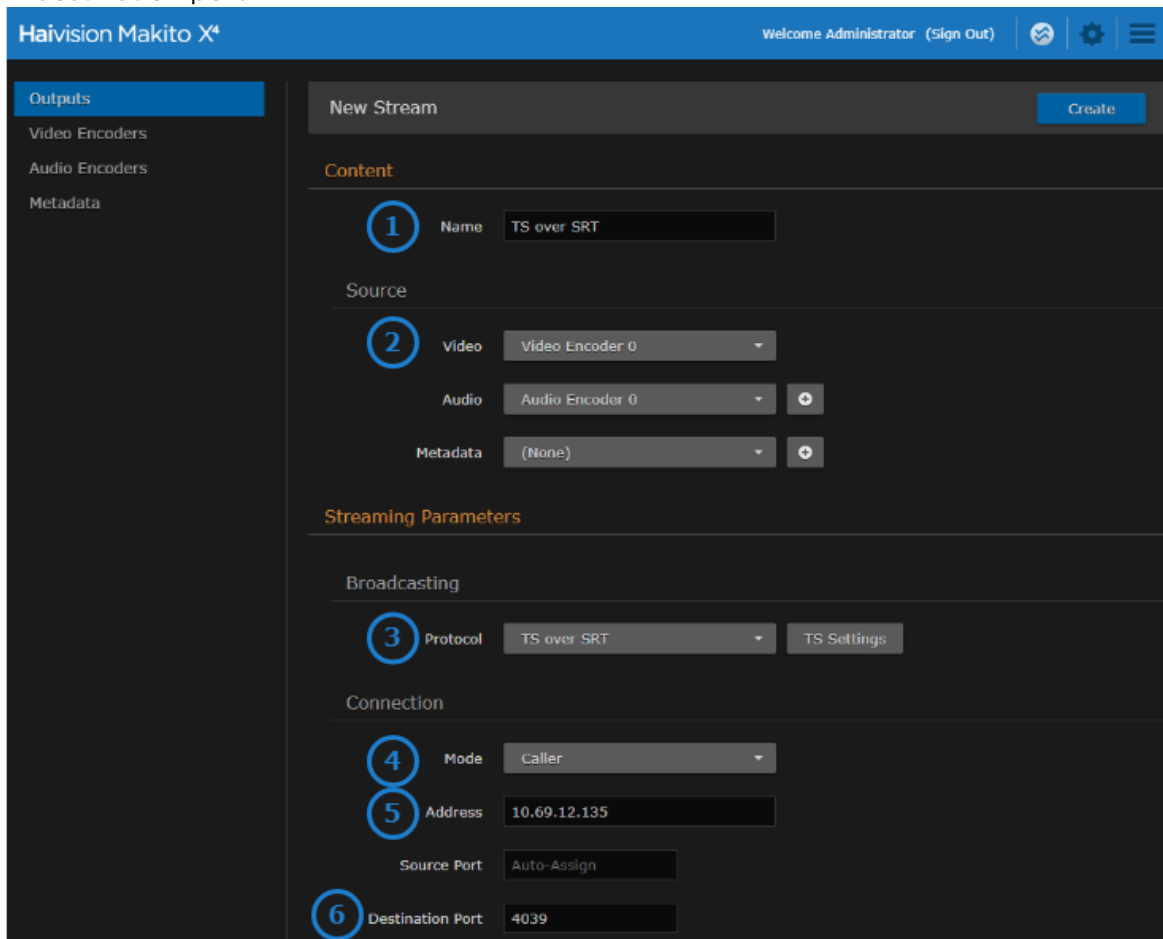
> ✅ **Tip**
>
> If needed, switch to the appropriate browser tab or enter the URL for the cloud-hosted gateway to acquire this information.

5. Click **Apply**.

Connecting the Source to the Cloud-Hosted Gateway

1. If you followed the steps in **Creating your Workspace (Optional)**, switch to the Gateway's browser tab. Else, enter the URL for the Media Gateway/SRT Gateway encoder web interface and sign in when prompted.
2. On the Route List screen, click the **Add Route** button.
3. When the Create Route screen opens:
   - Supply a (1) route name and check the (2) Start Once Created 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 set the (5) mode to Listener.
   - Enter the (6) port from the source encoder.
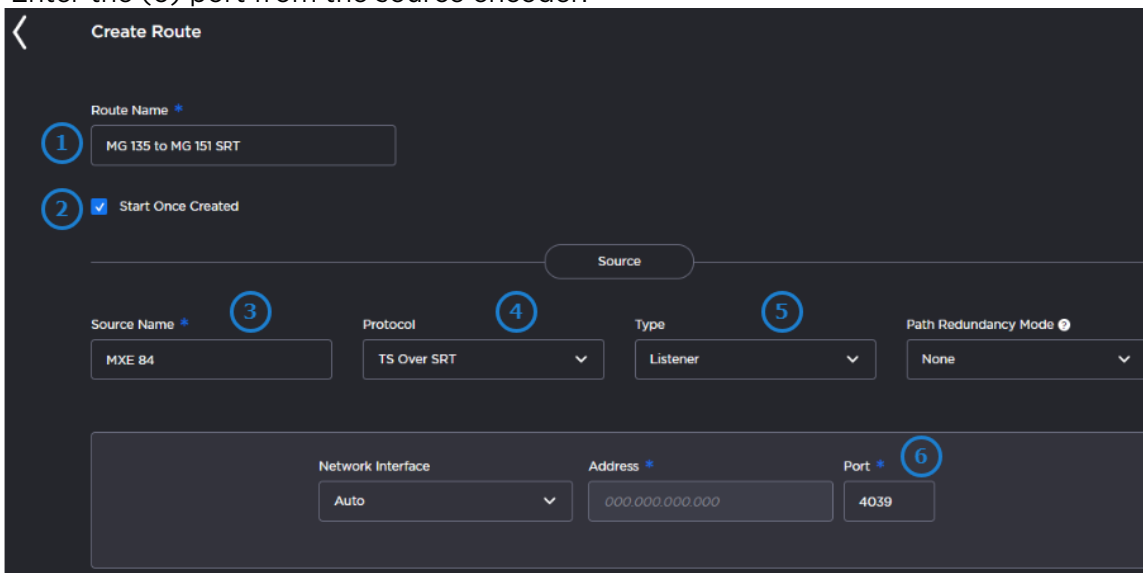
> ✅ **Tip**
>
> If needed, switch to the Makito X4 Encoder browser tab or enter the URL for the Makito X4 Encoder to acquire this information.

4. Click the **Add Destination** button.
5. In the New Destination dialog, enter the information for the LAN-based Gateway:
   - Provide a (1) name.
   - Change the (2) protocol to "TS over SRT" and change the (3) mode to "Caller."
   - Enter the (4) address and the (5) port of the destination.

> ⚠️ **Note**
>
> Protocols and types can have different configuration requirements. Data fields appear or disappear depending upon your choices. As just demonstrated, SRT protocols require an address and port when they are running in Caller mode.

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

6. When finished, click **Save**.
7. On the New Route screen, when finished, click **Create**.
8. On the Route List screen, expand the route to verify that the status indicators change to green.

Connecting the Gateway to the Remote Site's Makito X4 Decoder

1. Switch to the LAN-based Gateway browser tab or enter the URL for the LAN-based Gateway web interface.
2. Click **Add Route** button to add a new route.
3. In the New Route screen:
   - Supply a (1) route name and check the (2) Start Once Created checkbox so that the stream starts after creation.
   - In the Source section, provide a (3) source name, the (4) protocol of "TS over SRT", and the (5) mode to "Listener".
   - Enter the (6) port.

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

4. Click **Add Destination**.
5. In the Add Destination dialog, enter the information for the Decoder:
   - Provide a (1) name and select the (2) protocol as "TS over UDP".
   - Enter the (3) address and (4) port information for the destination.

6. When finished, click **Save**.
7. In the New Route screen, click **Apply**.

Connecting the Makito X4 Decoder

1. Switch to the Makito X4 Decoder tab or enter the URL for the Makito X4 Decoder web interface.
2. Click **Add Stream** to add the stream to the Makito X4 Decoder.
3. On the New Stream screen:
   - Enter a (1) name and the (2) protocol.
   - For this example, we are using unicast TS over UDP. So, you need to include the (3) type and (4) port information.
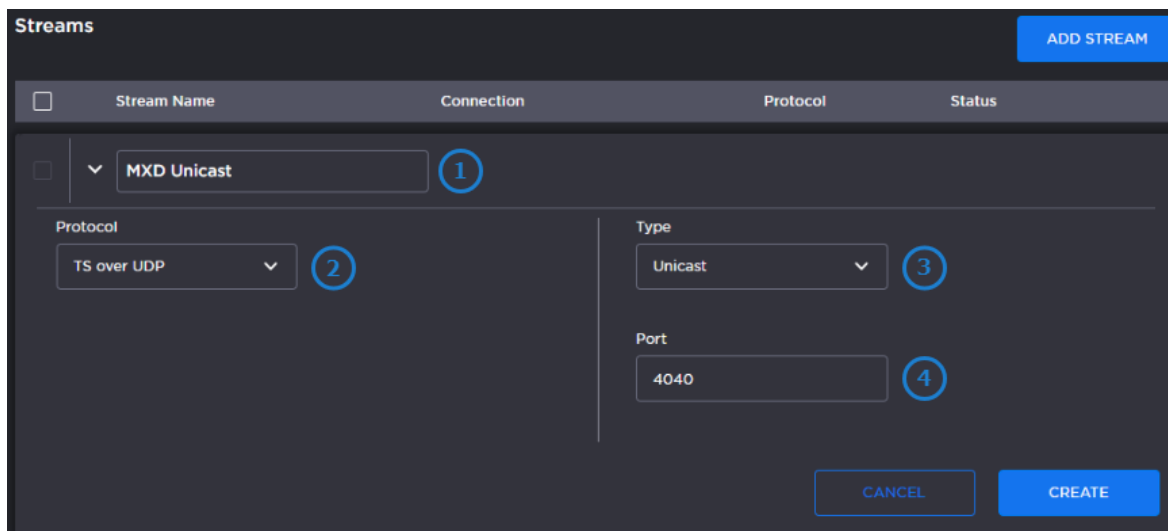
4. Click **Create**.
5. Repeat steps #2 and #3 as needed to define additional streams.
6. To ensure that everything is set up properly, verify that the streams have green status indicators on each device.

Status Indicators
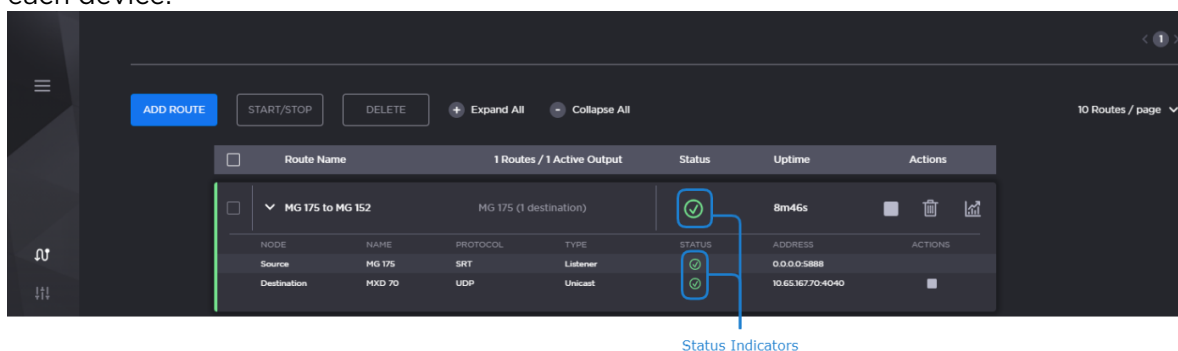
⚠ **Note**

Refer to your **Makito X4 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/SRT 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.
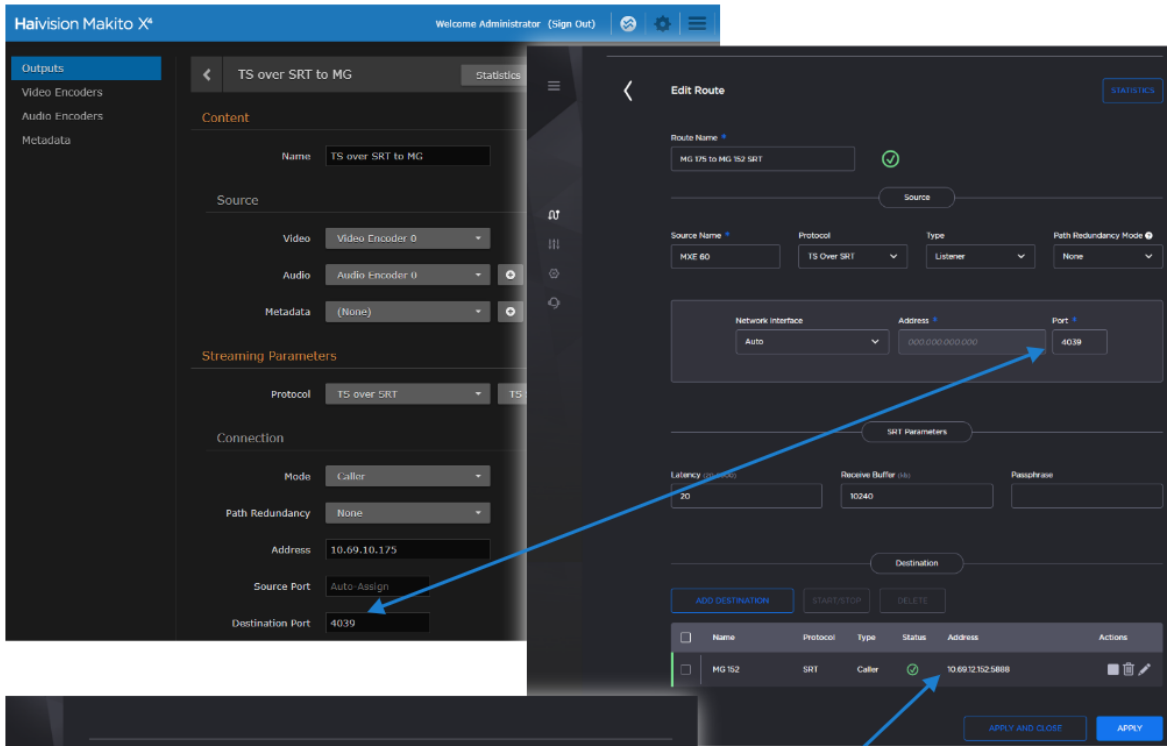
In turn, the stream is routed to a Media Gateway/SRT Gateway located behind the firewall at the remote office in Austin, Texas. The Gateway converts the SRT protocol to TS over UDP where it is ingested by the Makito X4 Decoder and displayed for viewing.
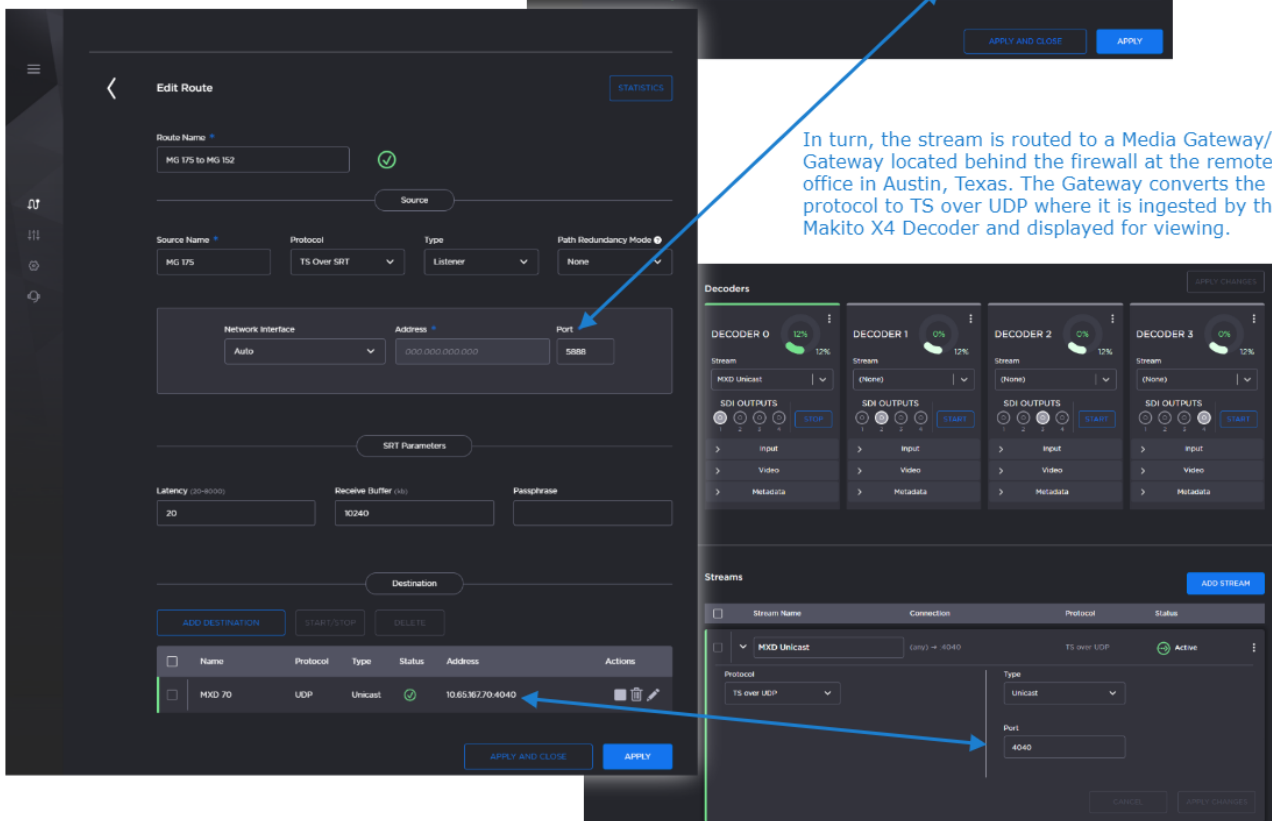
Working with Routes

> ⚠️ **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 **Route List**.
2. Click the **Add Route** button.
3. A Create Route screen appears for entering the desired settings for the route. The screen is divided into four sections as shown below.
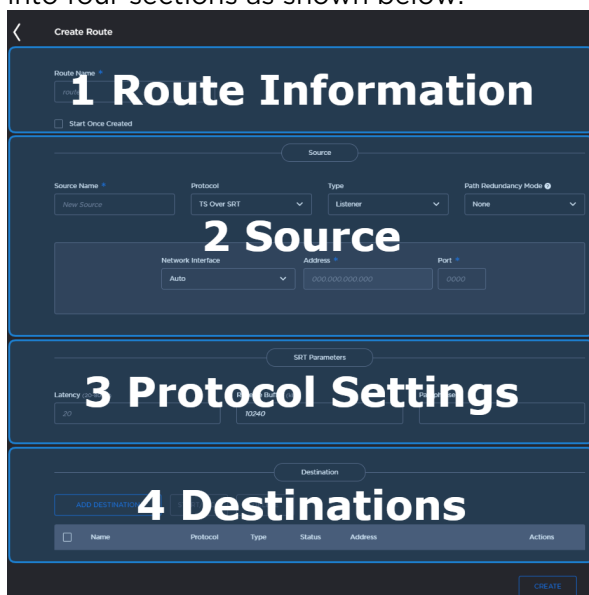
Further instructions and detailed descriptions for each setting are provided for each section, accessible in the following table

Section	Description
1	Route Information
2	Source
3	Protocol Settings (SRT only)
4	Destinations

4. When you have finished entering the required data, click the **Create** button to create the route.

You are returned to the Route List screen, and after a few seconds the new route appears. Click the ➤ button next to the new route to view specific source and destination details.

Section 1 Route Information

Creating a Channel

Step	Description
1	Name and Description
2	Source
3	Protocol Settings (SRT only)
4	Destinations

The following figure shows the Route Information section of the Route screen. The numbered callouts in the figure indicate the step number in this procedure.
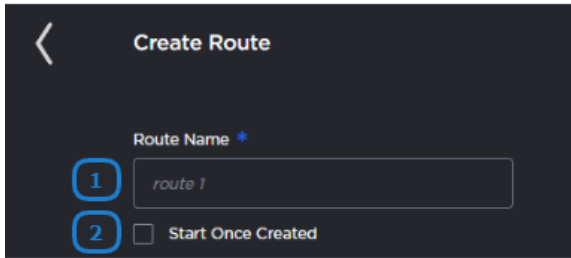
1. Enter the desired name for the route.
2. Select whether to automatically start the route after it is created.

> ✅ **Tip**
>
> If this checkbox is disabled, when subsequently starting the route, its destinations must be manually started.

Continue to Section 2 Source.

Section 2 Source

Creating a Channel	
Step	**Description**
1	Route Information
2	Source
3	Protocol Settings (SRT only)
4	Destinations

The available configuration options depend on the selected source streaming protocol.

TS over UDP   TS over SRT   TS over RTP   RTMP   RTSP

The following figure shows the Source section of the Route screen for a TS over UDP route. The numbered callouts in the figure indicate the step number in this procedure.
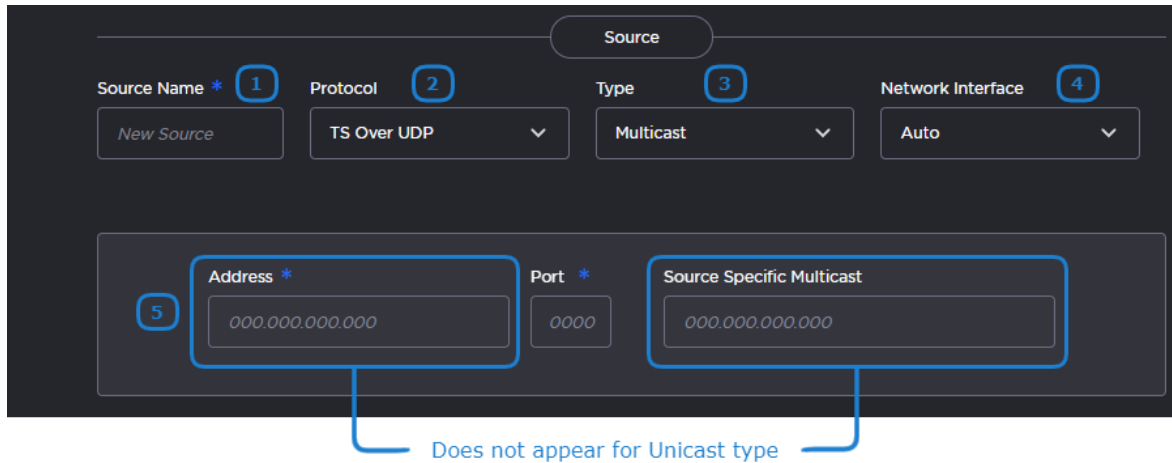
Does not appear for Unicast type

1. Enter the desired name for the source stream.

   > ✅ **Tip**
   >
   > Keep the name under 30 characters to have the entire name displayed in the Route List screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.

2. In the Protocol dropdown, select **TS over UDP**.
3. Select **Unicast** or **Multicast** in the Type dropdown.
4. Choose the desired network interface to use for this route in the dropdown. Available options depend on the hardware configuration.
5. If you chose Unicast in the previous step, enter the listening port number.
   If you chose Multicast in the previous step, enter the multicast IP address and listening port number. Also, optionally, enter the IGMP v3 source address in the Source Specific Multicast field.

   > ⚠ **Note**
   >
   > IGMPv3 Source Specific Multicast reception allows input streams to join a multicast group and filter the input streams based on a specific source IP address. Only streams originating from the specified source IP are forwarded to HMG/HSG, which allows HMG/HSG to quickly and easily select an input stream in environments with many sources sharing a common multicast IP. See **IETF RFC 3376** for more details.

As there are no additional protocol settings to configure, continue to **Section 4 Destinations**.

TS over UDP   **TS over SRT**   **TS over RTP**   **RTMP**   **RTSP**

The following figure shows the Source section of the Route screen for a TS over SRT route. The numbered callouts in the figure indicate the step number in this procedure.

1. Enter the desired name for the source stream.

   > ✅ **Tip**
   >
   > Keep the name under 30 characters to have the entire name displayed in the Route List screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.

2. In the Protocol dropdown, select **TS over SRT**.
3. Specify the SRT connection mode in the Mode dropdown:
   • 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.

4. If you chose Caller or Listener mode, select whether to use SRT Path Redundancy. If so, select the desired mode and use the **+**/**–** buttons next to each network address to add/subtract network paths when completing the following two steps. See **Using Path Redundancy with SRT Streaming** for more details.
   • Any (SRT Listener only) — Automatically use the path redundancy mode defined by SRT Caller.
   • Active-Active — Stream packets are sent on all defined network paths. The listener uses the first received stream packets and ignores the duplicate packets received from the other network paths. This mode maintains low latency at the expense of network bandwidth.
   • Active-Backup — Stream packets are sent only on the main network path. If the main path fails, one of the backup paths begins transmission of the stream. This mode saves network bandwidth at the expense of latency.
   • None — SRT Path Redundancy disabled.
5. Choose the desired Network Interface to use in the dropdown. Available settings depend on the hardware configuration.
6. If using SRT Listener mode, enter the listening port.
   If using SRT Caller or Rendezvous mode, enter the source stream address and port.

Continue to **Section 3 Protocol Settings**.

TS over UDP   **TS over SRT**   **TS over RTP**   **RTMP**   **RTSP**

The following figure shows the Source section of the Route screen for a TS over RTP route. The numbered callouts in the figure indicate the step number in this procedure.
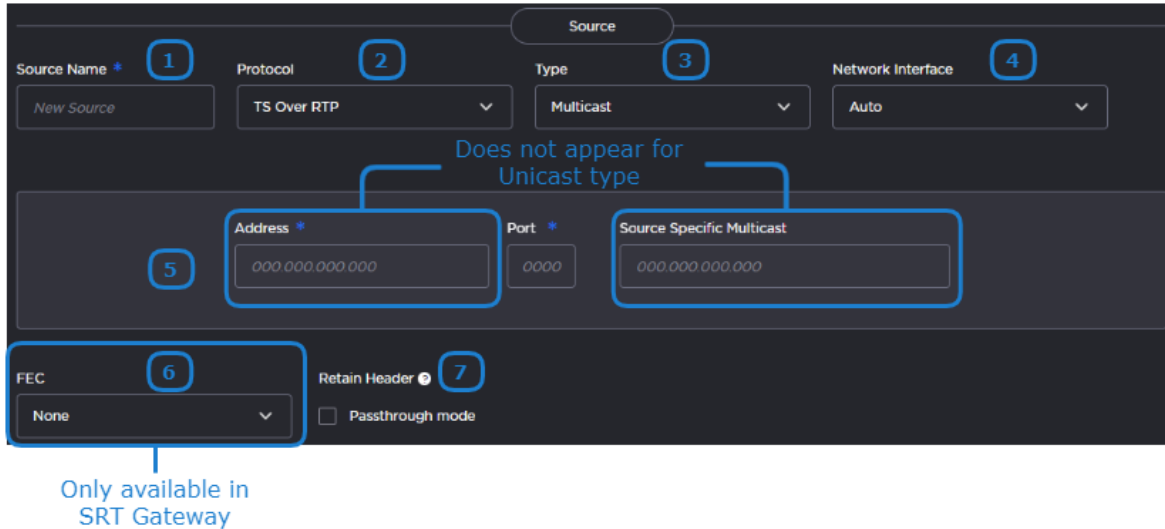
1. Enter the desired name for the source stream.

> ✅ **Tip**
>
> Keep the name under 30 characters to have the entire name displayed in the Route List screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.

2. In the Protocol dropdown, select **TS over RTP**.
3. Select **Unicast** or **Multicast** in the Type dropdown.
4. Choose the desired network interface to use for this route in the dropdown. Available options depend on the hardware configuration.
5. If you chose Unicast in a previous step, enter the listening port number.
   If you chose Multicast in a previous step, enter the multicast IP address and listening port number. Also, optionally, enter the IGMP v3 source address in the Source Specific Multicast field.

> ✅ **Tip**
>
> An even-numbered port is required for RTP, as recommended in RFC 3550. (The next odd-numbered port is typically reserved for RTCP messages.)

> ⚠️ **Note**
>
> IGMPv3 Source Specific Multicast reception allows input streams to join a multicast group and filter the input streams based on a specific source IP address. Only streams originating from the specified source IP are forwarded to HMG/HSG, which allows HMG/HSG to quickly and easily select an input stream in environments with many sources sharing a common multicast IP. See IETF RFC 3376 for more details.

6. Select whether PRO-MPEG FEC is enabled or not.

> ⚠️ **Note**
>
> PRO-MPEG FEC is available only on Haivision SRT Gateway.

7. If you plan to tunnel the RTP stream through SRT, check the Retain Header > Passthrough mode checkbox. See **Tunnelling an RTP Stream Through SRT** for more details.

> ⚠️ **Note**
>
> PRO-MPEG FEC is not supported when Passthrough mode is enabled.

As there are no additional protocol settings to configure, continue to **Section 4 Destinations**.

| TS over UDP | TS over SRT | TS over RTP | **RTMP** | RTSP |

The following figure shows the Source section of the Route screen for an RTMP route. The numbered callouts in the figure indicate the step number in this procedure.
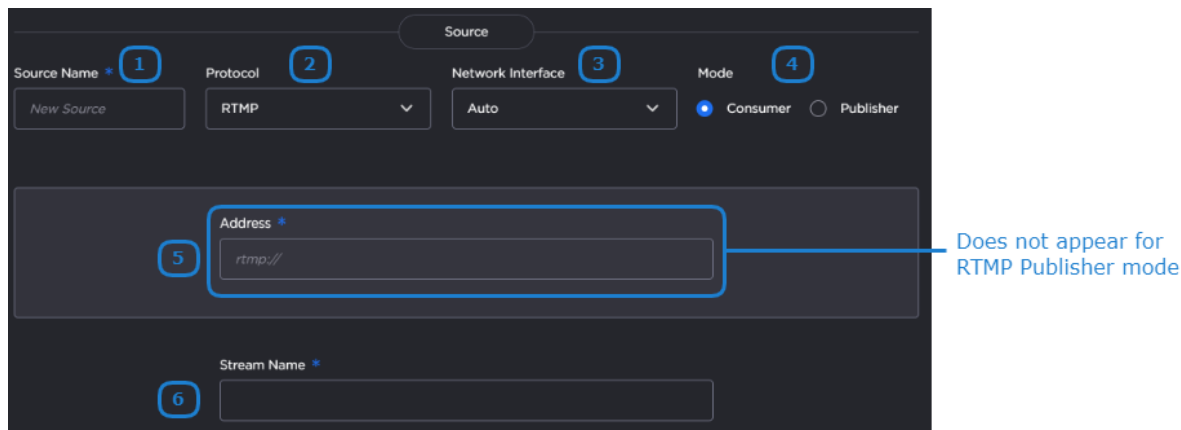
1. Enter the desired name for the source stream.

> ✅ **Tip**
>
> Keep the name under 30 characters to have the entire name displayed in the Route List screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.

2. In the Protocol dropdown, select **RTMP**.
3. Choose the desired network interface to use for this route in the dropdown. Available options depend on the hardware configuration
4. Select the mode for connection to the RTMP stream:
   • Consumer — Stream available for Media Gateway/SRT Gateway to access on an RTMP server.
   • Publisher — Stream sent directly to the Media Gateway/SRT Gateways's IP address. See **Connecting an RTMP Publisher Source** for further details regarding RTMP Publisher mode.
5. If using RTMP Consumer mode, enter the source stream address, including the port number.

> ⚠ **Important**
>
> This is the RTMP source address, not the address of your HMG/HSG.

6. Enter the RTMP stream name.

Continue to **Section 3 Protocol Settings**.

TS over UDP   **TS over SRT**   **TS over RTP**   **RTMP**   **RTSP**

The following figure shows the Source section of the Route screen for an RTSP route. The numbered callouts in the figure indicate the step number in this procedure.
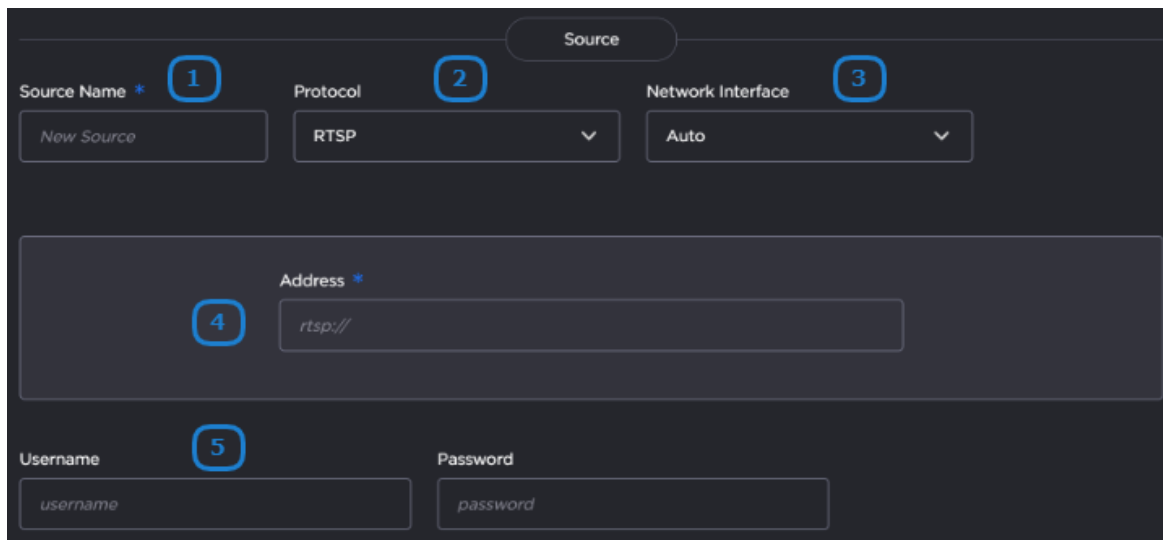
1. Enter the desired name for the source stream.

> ✅ **Tip**
>
> Keep the name under 30 characters to have the entire name displayed in the Route List screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.

2. In the Protocol dropdown, select **RTSP**.
3. Choose the desired network interface to use for this route in the dropdown. Available options depend on the hardware configuration.
4. Enter the source stream address, including the port number.
5. Specify the username and password for the RTSP stream.

> ⚠ **Note**
>
> Depending on the stream, the username/password may not be required.

Continue to **Section 3 Protocol Settings**.

Section 3 Protocol Settings

Creating a Channel	
Step	**Description**
1	Route Information
2	Source
3	Protocol Settings (SRT only)
4	Destinations

If TS over SRT is chosen in Section 2 Source, follow the instructions below for your chosen stream protocol. For all other protocols, continue to Section 4 Destinations as there are no additional protocol settings.

The following figure shows the SRT Parameters section of the Create Route screen. The numbered callouts in the figure indicate the step number in this procedure.
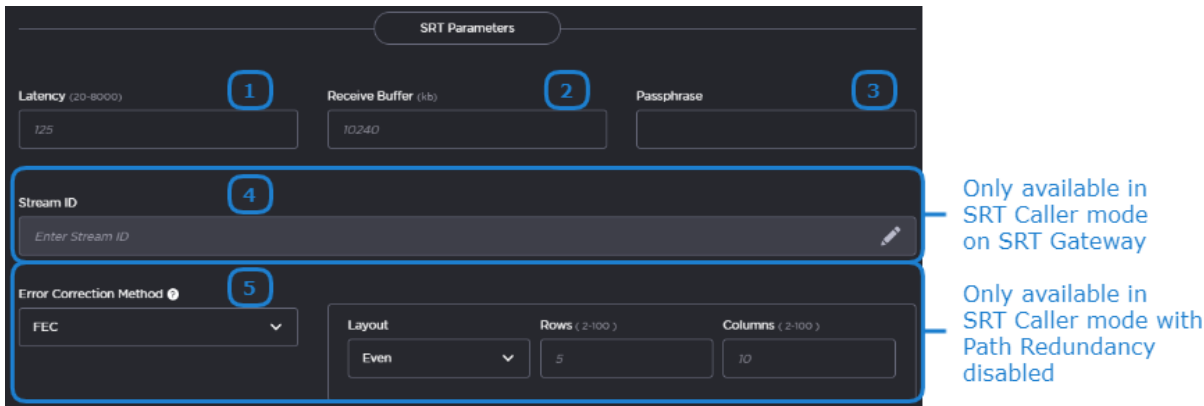
1. Enter the desired latency. This specifies the SRT receiver buffer that permits lost packet recovery. The size of this buffer adds up to the total latency. A minimum value must be 3 times the round-trip-time (RTT). Range = 20–8000 ms.

   > ⚠ **Note**
   >
   > Latency is for the SRT protocol only and does not include the capture, encoding, decoding, and display processes of the endpoint devices.

2. *(For advanced users only.)* Enter the desired Receive Buffer Size. High-bandwidth (≥60 Mbps), high-latency streams may experience video dropouts due to the default receive buffer size. If you notice this issue for your stream, use the following formulas to guide you in setting an appropriate buffer size, where:
   - MTU size is defined at the stream's source.
   - Bitrate and negotiated latency are found on the route statistics page while the route is running. (See Viewing a Route's Statistics.) The negotiated latency is not necessarily the value set in Step #2.

MTU Size	Suggested Receiver Buffer Size (in kByte)
1000–1500	(Bitrate in kbps ÷ 8) × negotiated latency in seconds × 1.5

MTU Size	Suggested Receiver Buffer Size (in kByte)
750–1000	(Bitrate in kbps ÷ 8) × negotiated latency in seconds × 1.7
< 750	(Bitrate in kbps ÷ 8) × negotiated latency in seconds × 2.0

3. If using Encryption on any destinations, enter the desired passphrase to protect the stream. Must be between 10 to 79 UTF8 characters.
4. If you have a Haivision SRT Gateway, for SRT Caller mode click the ✏ icon to open the Stream ID editor. In the editor:
   a. Select the desired Stream ID format.
      • If Default Stream ID format is selected, enter the Resource Name and User Name. The resulting Stream ID appears below.
      • If Custom Stream ID format is selected, enter the desired text string for the Stream ID.
   b. Click the Apply button to close the Stream ID editor.
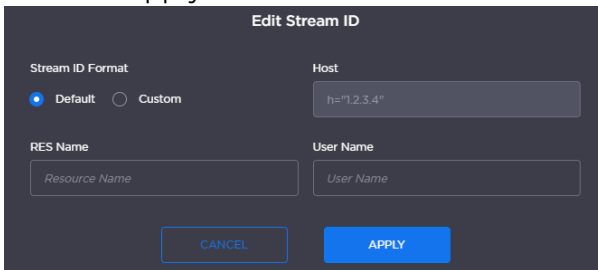
5. In SRT Caller mode with Path Redundancy disabled, select the Error Correction Method: ARQ (Automatic Repeat Request), FEC, or FEC+ARQ. See **Choosing an Error Correction Method for SRT Streams** for more information on using SRT FEC. When FEC or FEC+ARQ is selected:
   a. Select the Layout: Even or Staircase.
   b. Enter the number of rows and columns in the FEC matrix.

Continue to **Section 4 Destinations**.

Section 4 Destinations

Creating a Channel	
Step	**Description**
1	**Route Information**
2	**Source**
3	**Protocol Settings** (SRT only)
4	Destinations

Depending on the desired protocol for the destination, follow the steps below.

TS over UDP   TS over SRT   TS over RTP   HLS

1. On the Route screen click the **Add Destination** button. The following dialog appears, with required fields identified with a blue asterisk. The numbered callouts in the figure indicate the step number in this procedure.
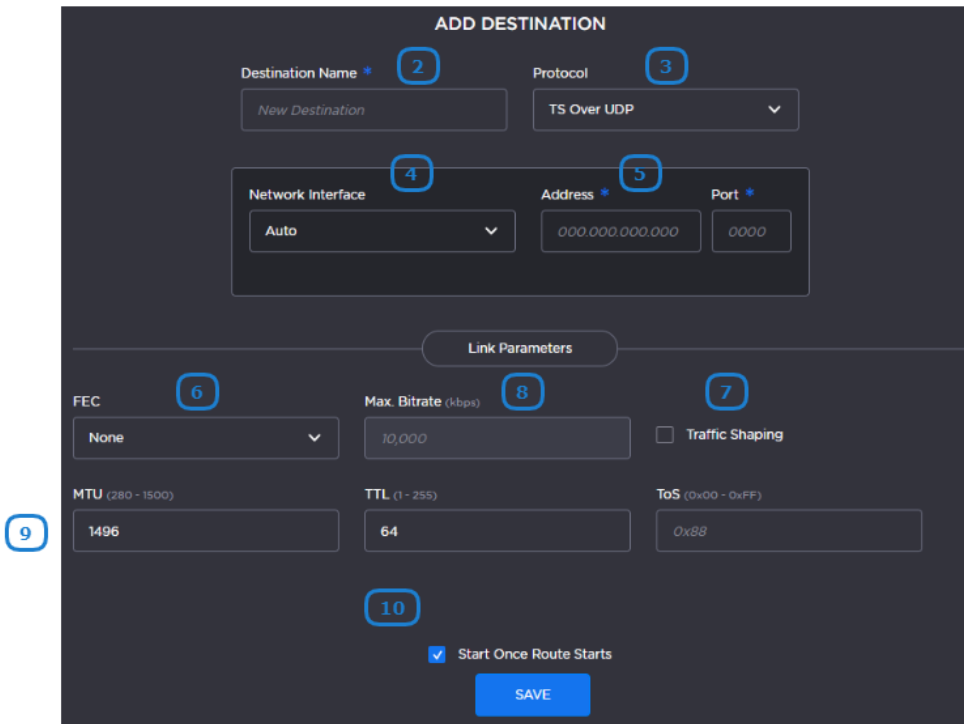
2. Enter the desired name.

> ✅ **Tip**
>
> Keep the name under 30 characters to have the entire name displayed in the Route List screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.

3. Select **TS over UDP** from the Protocol drop-down menu.
4. Select the desired network interface to use for the destination in the dropdown. Available options depend on the hardware configuration.
5. Enter the destination address and port number.
6. Enable or disable Forward Error Correction (FEC).

> ⚠️ **Note**
>
> VF FEC is a proprietary FEC and is not inter-operable with devices outside of the Haivision family.

7. 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. Traffic Shaping controls the outgoing stream so that the inter-packet time is constrained, to reduce the probability that TCP packets are dropped in a session.

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

8. If traffic shaping is enabled in the previous step, enter the Maximum Bitrate in kbps.
9. Enter values for MTU, TTL, ToS, and Latency:

- MTU (Maximum Transmission Unit) — The maximum allowed size of IP packets for the outgoing data stream. Range: 280-1500.
- TTL (Time-to Live for stream packets) — The number of router hops the stream packet is allowed to travel/pass before it must be discarded. Range: 1-255.
- ToS (Type of Service) — This value will be assigned to the Type of Service field of the IP Header for the outgoing streams. Range: 0x00-0xFF.

10. Click the **Save** button.

TS over UDP   **TS over SRT**   TS over RTP   HLS

> ⚠ **Important**
>
> The System 100 Generation 2 appliance is not capable of sending a single 50-Mbps MPEG-TS source to two SRT destinations simultaneously (i.e., two 50-Mbps streams for 100-Mbps total output).

1. On the Route screen click the **Add Destination** button. The following dialog appears (depending on which SRT type you select in step 4), with required fields identified with a blue asterisk. The numbered callouts in the figure indicate the step number in this procedure.

SRT Caller	SRT Listener and Rendezvous
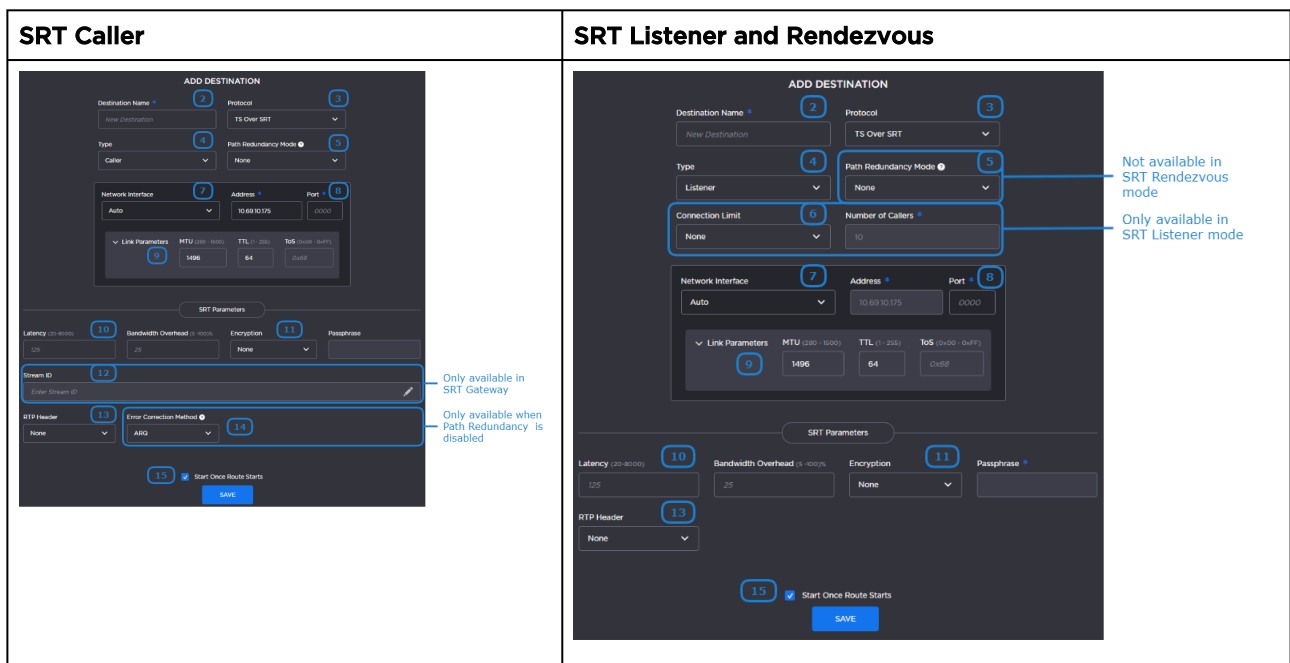
2. Enter the desired name.

> ✅ **Tip**
>
> Keep the name under 30 characters to have the entire name displayed in the Route List screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.

3. Select **TS over SRT** from the Protocol drop-down menu.
4. Select the SRT mode: **Listener**, **Caller**, or **Rendezvous**.
5. If you chose Caller or Listener mode, select whether to use SRT Path Redundancy. If so, select the desired mode and use the **+/–** buttons next to each network address to add/subtract

network paths when completing the following three steps. See **Using Path Redundancy with SRT Streaming** for more details.

6. If you chose Listener mode, select whether that you would like a Caller connection limit. Use a limit if you are concerned about bandwidth consumption for your route.

7. Select the desired network interface to use for the destination in the dropdown. Available options depend on the hardware configuration.

8. If you selected Listener mode, enter the listening port number.
   If you selected Caller or Rendezvous mode, enter the destination address and port number.

9. Enter values for MTU, TTL, and ToS:
   • MTU (Maximum Transmission Unit) — The maximum allowed size of IP packets for the outgoing data stream. Range: 280-1500.
   • TTL (Time-to Live for stream packets) — The number of router hops the stream packet is allowed to travel/pass before it must be discarded. Range: 1-255.
   • ToS (Type of Service) — This value will be assigned to the Type of Service field of the IP Header for the outgoing streams. Range: 0x00-0xFF.

10. In the SRT Parameters section, enter the values for Latency and Bandwidth Overhead:
    • Latency — 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). Range = 20-8000 ms.
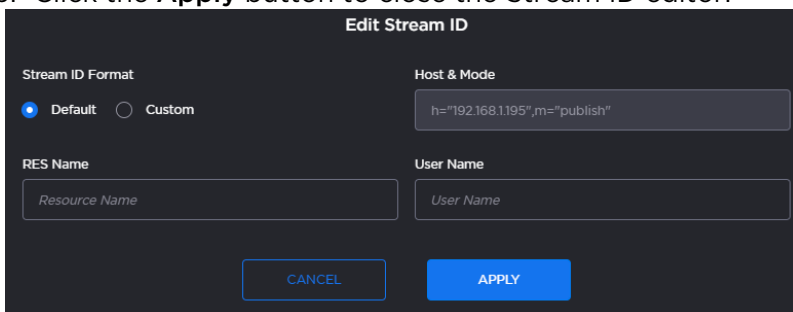
    > ⚠ **Note**
    >
    > Latency applies to the SRT protocol only and does not include the capture, encoding, decoding and display processes of the end-point devices.

    • Bandwidth Overhead — The percentage of the average bandwidth that is used to accommodate SRT controls as well as recovery of lost packets. (The "average bandwidth" is an internal measurement of the outbound traffic, on a per stream basis.) Range = 5-100% (default value is 25%).

    > ⚠ **Note**
    >
    > SRT streams may temporarily overshoot the defined bandwidth overhead limit.

11. Enable or disable AE128 or AE256 encryption. If enabled, enter the passphrase.

12. If you have a Haivision SRT Gateway, for SRT Caller mode click the 🖉 icon to open the Stream ID editor. In the editor:
    a. Select the desired Stream ID format.
       • If Default Stream ID format is selected, enter the Resource Name and User Name. The resulting Stream ID appears below.
       • If Custom Stream ID format is selected, enter the desired text string for the Stream ID.
    b. Click the **Apply** button to close the Stream ID editor.

13. If you plan to tunnel an RTP stream through SRT and your source RTP stream has its respective Retain Header checkbox enabled, check the RTP Header checkbox to transfer RTP headers through this SRT destination. See **Tunnelling an RTP Stream Through SRT** for more details.

14. If you chose SRT Caller mode and Path Redundancy is disabled, select the Error Correction Method: ARQ, FEC, or FEC+ARQ. See **Choosing an Error Correction Method for SRT Streams** for more information on using SRT FEC. When FEC or FEC+ARQ is selected:
    a. Select the Layout: Even or Staircase.
   b. Enter the number of rows and columns in the FEC matrix.
15. Click the **Add** button.

TS over UDP   **TS over SRT**   **TS over RTP**   **HLS**

1. On the Route screen click the **Add Destination** button. The following dialog appears, with required fields identified with a blue asterisk. The numbered callouts in the figure indicate the step number in this procedure.

2. Enter the desired name.

> ✅ **Tip**
>
> Keep the name under 30 characters to have the entire name displayed in the Route List screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.

3. Select **TS over RTP** from the Protocol drop-down menu.
4. Select the desired network interface to use for the destination in the dropdown. Available options depend on the hardware configuration.
5. Enter the destination address and port number.

> ✅ **Tip**
>
> An even-numbered port is required for RTP, as recommended in RFC 3550. (The next odd-numbered port is typically reserved for RTCP messages.)

6. Enable or disable PRO-MPEG Forward Error Correction (FEC).

> ⚠ **Note**
>
> PRO-MPEG FEC is available only on Haivision SRT Gateway.

> ⚠ **Important**
>
> - When PRO-MPEG is selected and Level A is selected in step 10, the next even numbered port following the port specified in Step 4 is allocated to the column FEC packets.
> - When PRO-MPEG is selected and Level B is selected in step 10, the two even numbered ports following the port specified in Step 4 are allocated to the column and row FEC packets, respectively.

7. 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. Traffic Shaping controls the outgoing stream so that the inter-packet time is constrained, to reduce the probability that TCP packets are dropped in a session.

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

8. If traffic shaping is enabled in the previous step, enter the Maximum Bitrate in kbps.
9. Enter values for MTU, TTL, and ToS:
   - MTU (Maximum Transmission Unit) — The maximum allowed size of IP packets for the outgoing data stream. Range: 280-1500.
   - TTL (Time-to Live for stream packets) — The number of router hops the stream packet is allowed to travel/pass before it must be discarded. Range: 1-255.
   - ToS (Type of Service) — This value will be assigned to the Type of Service field of the IP Header for the outgoing streams. Range: 0x00-0xFF.
10. If you plan to tunnel an RTP stream through SRT and your original RTP stream has its respective Retain Header checkbox enabled, check the Retain Header > Passthrough Mode checkbox to use the original RTP headers for this destination. See **Tunnelling an RTP Stream Through SRT** for more details.
11. For Haivision SRT Gateway, if PRO-MPEG FEC is enabled in step 6, enter the PRO-MPEG values:
    - Level — The level of FEC protection: A (Column only) uses the column FEC stream, or B (Row and Column) uses both column and row FEC streams.
    - Block Aligned — Specifies the type of FEC matrix scheme.Check this checkbox to align the FEC blocks in the matrix structure (i.e., sequential columns within a group start on the same row), see Annex C of SMPTE 2022-1. If left unchecked, the blocks are a staggered series of FEC packets (i.e., each column starts on the row below the row on which the previous column started), see Annex B of SMPTE 2022-1.
    - Columns — The number of columns in the FEC matrix.
    - Rows — The number of rows in the FEC matrix.
12. Click the **Add** button.

TS over UDP   TS over SRT   TS over RTP   HLS

1. On the Route screen click the **+Destination** button. The following dialog appears, with required fields identified with a blue asterisk. The numbered callouts in the figure indicate the step number in this procedure.

2. Enter the desired name.

> ✅ **Tip**
>
> Keep the name under 30 characters to have the entire name displayed in the Route List screen. Longer names are still visible, but you must hover your cursor over the name for a popup to appear displaying the entire name.

3. Select **HLS** from the Protocol drop-down menu.
4. Enter the 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 (See **this link**). 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.

5. Enable or disable HLS v4 Variant Playlists. If the destination does not support variant playlists, deselect this checkbox.
6. Enable or disable HLS Encryption (AES-128 using 16-octet keys).
7. If HLS encryption is enabled, in Segments/Keys enter how often a new random key file is inserted. That is, a new random key file is inserted every *n* media segments (key rotation). Each group of *n* segments is encrypted using a different key.

8. Click the **Add** button.

Return to Step #4 in Creating a Route.

Editing a Route

To edit a route:

1. On the Route List screen, click the **Route Name** for the route you want to edit.
2. In the the Edit Route screen, adjust the settings as desired.
3. Click the **Apply and Close** button to save the new settings and return to the Route List screen.

Related Topics

- Creating a Route
- Starting, Stopping, and Deleting a Route

Starting, Stopping, and Deleting a Route

> ⚠️ **Note**
>
> When stopping a route, the current state of the destinations is preserved. For example, if a destination is stopped prior to its route being stopped and the route is restarted, the destination stays stopped.

To start, stop, or delete a route:

1. On the Route List screen, locate the desired route and click **Start/Stop** or **Delete** icon in the listing.

-or-
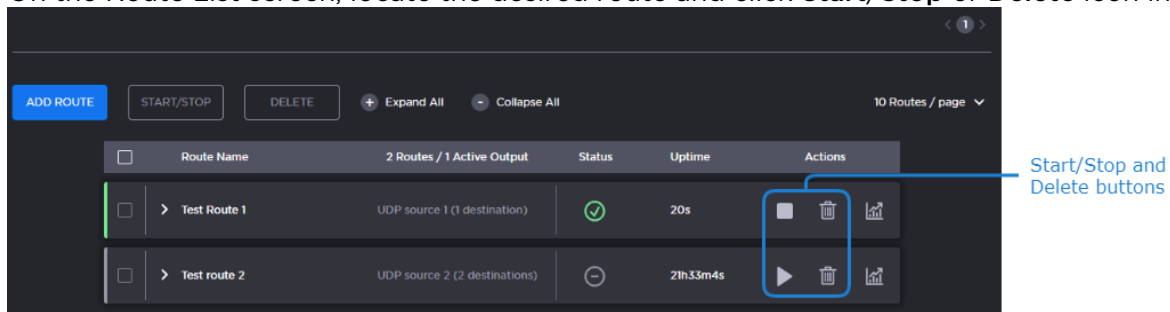
Check the checkboxes next to the routes you wish to start, stop, or delete and click the **Start/Stop** or **Delete** button.
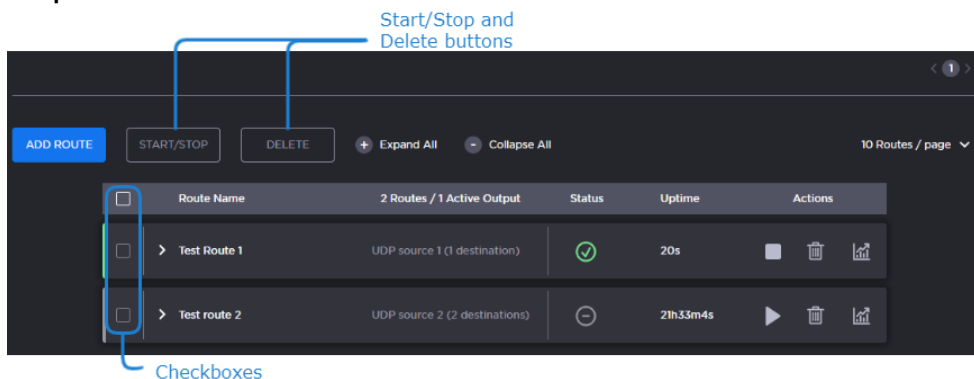
2. In the Confirm Action dialog, click the **Confirm** button.

> ✅ **Tip**
>
> If you select multiple routes with varying start/stop statuses and you click the **Start/Stop** button, the routes toggle their status.

Related Topics

- **Creating a Route**
- **Editing a Route**
- **Viewing a Route's Statistics**

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 Route List screen, click the 📈 icon of the route you are interested in.
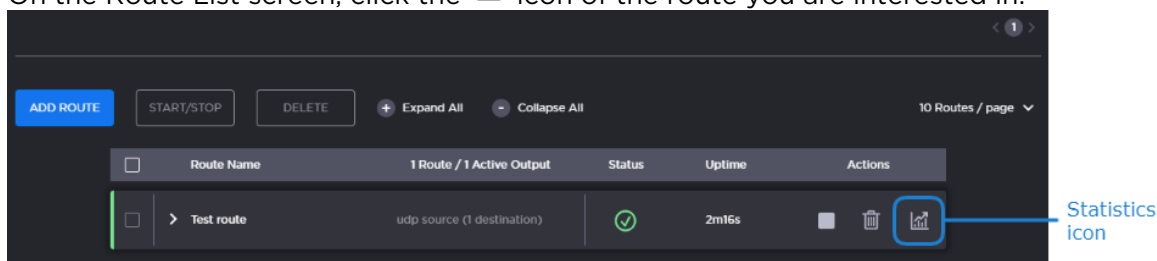
2. When the Statistics page appears, you can view the pertinent data for the routes' source and destinations. See **Stream Statistics Field Descriptions** for detailed descriptions of each statistic.

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.

> ✅ **Tip**
>
> For SRT Listener streams, you can view the statistics for each connected client by selecting the Client in the dropdown menu, as shown in the following figure.
>
>

Other elements are available on the as shown in the following figure and bullet list:

Download statistics button

Refresh rate drop-down menu

Graph icon opens a real-time chart of the data. Only available for SRT sources/ destinations.

- To download a JSON file containing route statistics data from the past 24 hours, click the **Download Data** button.

> ✅ **Tip**
>
> After clicking the **Download Data** button, the download may take a few seconds to begin.

- To change the refresh rate, click the Refresh Rate drop-down menu.
- To view the data graphically for SRT sources or destinations, click the 📈 icon for the desired route. A separate Statistics Graph View window opens, displaying the data numerically and graphically for that route. This window remains open until you manually close it.
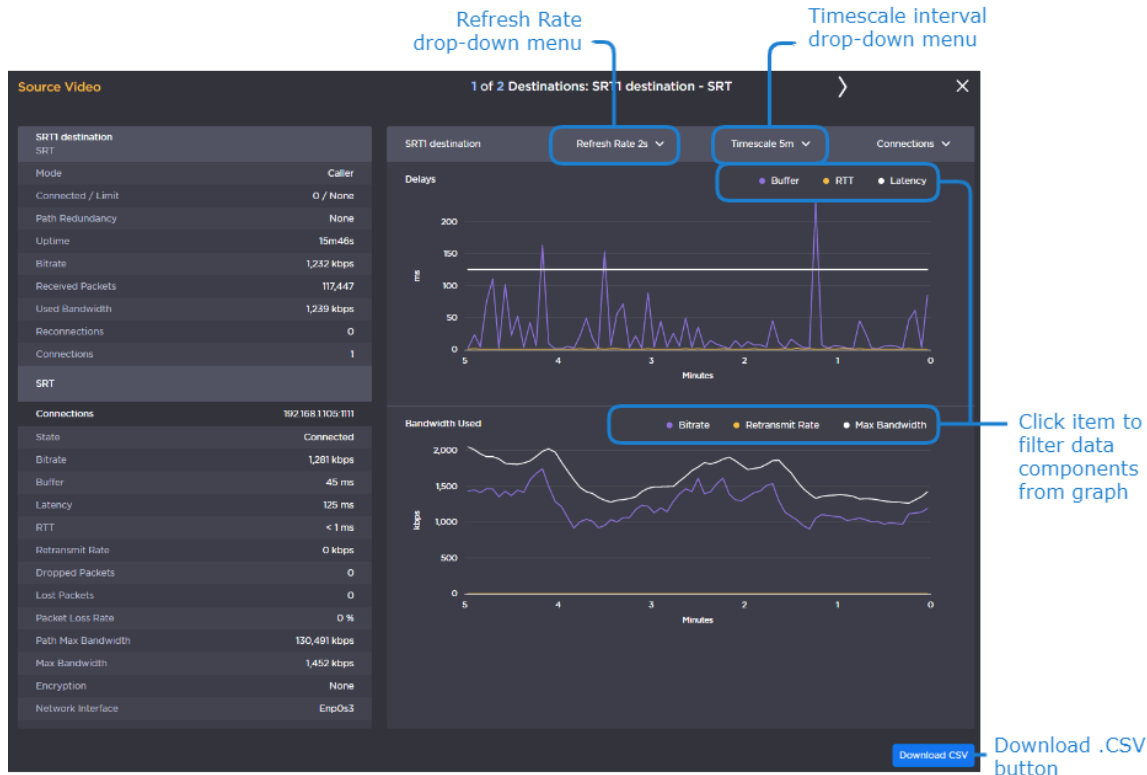
- To save the data for use with another application (such as a spreadsheet), click the **Download CSV** button. Typically, this downloads the data in a comma-separated values text file. For Safari browsers, this displays the file in a new window. Right-click the browser window and select "Save Page as…" to download the file.
- 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 1 day.
  - Clicking an item in each legend to display/hide the corresponding data components.
- Hovering your mouse cursor over the graph, reveals the time and values of the selected data point.
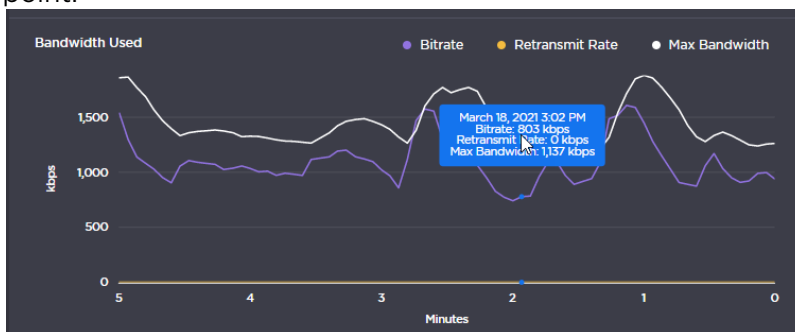
- For SRT Listener streams, you can view the statistics graph for each connected client by selecting the Client in the dropdown menu, as shown in the following figure:
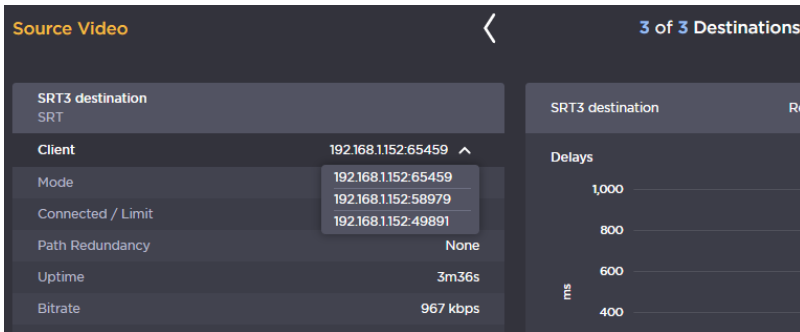
Related Topics

- **Creating a Route**
- **Starting, Stopping, and Deleting a Route**
- **Reports (Logs)**

Stream Statistics Field Descriptions

The following tables list the available stream statistics fields.

General   **SRT**   **Pro-MPEG FEC**

General

Statistic	Description/Values
State	The current operating status of the stream, either Disconnected, Connecting, Connection established, or Connected.
Mode	For UDP or RTP: Unicast or Multicast For HLS: HLS For SRT: Caller, Listener, or Rendezvous
Uptime	The elapsed running time of the stream.
Bitrate	The stream bitrate (in kbps).
Received Packets (Source) Sent Packets (Destination)	Number of packets received/sent for that stream.
Used Bandwidth	Bandwidth used.
Reconnections	Number of signal losses.
User NICs	Number of network interfaces used.

General   **SRT**   **Pro-MPEG FEC**

SRT

Statistic	Description/Values
Connections/Limit	Shows the number of SRT Caller clients connected to an SRT Listener stream and the connection limit defined in the SRT Listener destination.
Path Redundancy	Shows the defined path redundancy mode for the route.
Buffer	Decoder buffer in milliseconds. SRT decoder buffers are the received stream packets waiting to be decoded. This statistic shows the portion of the buffers up to the first missing packet. In other words, the remaining time to transmit the missing packet before it's too late. The level of the buffer in absence of packet loss is just below the latency value. In presence of packets loss, it is between 0 and the latency value. ✅ **Tip** If the Buffer goes to 0 often, then there is most likely insufficient BW to support the desired bitrate. In this case, decrease your bitrate. If the Buffer occasionally goes to 0, then the SRT Latency should be increased.
Latency	Maximum of the decoder and encoder configured Latency. For example: • Encoder Configured SRT Latency = 750 ms • Decoder Configured SRT Latency = 20 ms • The SRT Stats Latency (which is the current SRT connection applied Buffering Latency) = 750 (largest of the two). At startup, handshake exchanges the value configured on both sides and the largest one is selected. The decoder default is set to the minimum (20ms), so the latency value can be completely controlled from the encoder side.
RTT	Measured round-trip time. Round Trip Time (RTT) is the time it would take for a packet to travel from a specific source to a specific destination and back again. In SRT, this is measured as the time it takes for the destination device to send an acknowledgment (ACK) packet, and then receive a corresponding confirmation (ACKACK) packet.
FEC/FEC+ARQ	(SRT Caller mode only) If either FEC mode is enabled: Active.
FEC Layout	(SRT Caller mode only) FEC layout type: Even or Staircase.
FEC Rows/Columns	(SRT Caller mode only) Number of FEC rows and columns.

Other SRT statistics are available depending on whether the route is a source route or a destination route, as described below.

SRT Source   SRT Destination

SRT Source

Statistic	Description/Values
Lost Rate	Rate at which the source route is receiving lost packets in bits/s. See the following Lost Packets description for more details.

Statistic	Description/Values
Lost Packets	Number of SRT packets reported missing on the UDP connection. For each "hole" detected in the packet sequence, a request to re-transmit the lost packet is sent to the sender. This lost packet may (or may not) be re-covered by the re-transmit request. ⚠️ **Note** This is the raw number of packets dropped by the network. Most are recovered by retransmission at the source and so do not necessarily result in any artifacts.
Packet Loss Rate	SRT packet loss rate, expressed as a percentage of packets lost with respect to packets sent. The SRT on the sender side cannot deliver the packets within the defined latency time and dropped the packet. This occurs when the packets cannot be transmitted fast enough due to low latency, not enough bandwidth overhead, etc.
Skipped Packets	Packets that have arrived too late, or that never arrive at all from the receiver. If the "time to play" for a packet has passed, and it has either not arrived or arrives after the content it is associated with has already played, that packet is reported as "skipped". Usually this results in some type of video artifact (a replayed frame or video blocking). This is the raw number of packets skipped and are not recoverable by the SRT protocol. • If this statistic increments slowly, the best thing to do is increase the SRT latency. • If this statistic increments in large jumps, the best thing to do is lower your video bitrate or increase your overhead if you have available bandwidth. ⚠️ **Note** The skipped packets value from the receiver does not correlate to the dropped packets value from the sender, as they count different types of irrecoverable packets.
Encryption	SRT encryption type: None, AES128, or AES256.
Decryption	SRT decryption state: Active, Initializing, Inactive (no passphrase), Inactive (invalid passphrase).
Network Interface	Name of network interface used.

SRT Source   **SRT Destination**

SRT Destination

Statistic	Description/Values
Retransmit Rate	Rate at which the destination route is resending lost packets in bits/s.
Packet Loss Rate	SRT packet loss rate, expressed as a percentage of packets lost with respect to packets sent. The SRT on the sender side cannot deliver the packets within the defined latency time and dropped the packet. This occurs when the packets cannot be transmitted fast enough due to low latency, not enough bandwidth overhead, etc.

Statistic	Description/Values
Dropped Packets	Number of packets reported missing by the SRT sender, as the output queue has overflowed. The most likely cause for this is the system is overloaded and cannot process the data fast enough. This is the raw number of packets dropped and are not recoverable by the SRT protocol. ⚠ **Note** The skipped packets value from the receiver does not correlate to the dropped packets value from the sender, as they count different types of irrecoverable packets.
Max Bandwidth	Maximum bandwidth used by the source device for this SRT stream (i.e. the current total of audio/video bit rate plus ancillary data plus the SRT bandwidth overhead).
Path Max Bandwidth	An estimate of the maximum path/link bandwidth as viewed from the destination.
Encryption	SRT encryption type: None, AES128, or AES256.
Network Interface	Name of network interface used.

General   **SRT**   **Pro-MPEG FEC**

Pro-MPEG FEC

> ℹ️ **Note**
>
> PRO-MPEG FEC is available only on Haivision SRT Gateway.

Statistic	Description/Values
Lost Packets	Number of lost FEC packets.
Recovered Packets	Number of recovered FEC packets.
Unrecovered Packets	Number of unrecovered FEC packets.
Reordered Packets	Number of reordered FEC packets.
Level	The level of FEC protection: • A (Column only): uses the column FEC stream. • B (Row and Column): uses both column and row FEC streams.
Block Aligned	The type of FEC matrix scheme: • True: Sequential columns within a group start on the same row. • False: Each column starts on the row below the row on which the previous column started.
Columns/Rows	Number of columns and number of rows are the dimensions of the FEC matrix.

Working with Destinations

> ⚠️ **Note**
>
> Stopping a route saves the current state of the destinations and stops all destinations for the route. Starting a route resumes the saved state of the destinations.

Editing the Destination

To change the Destination settings:

1. On the Route List 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 **Section 4 Destinations** for definitions of the fields.

4. Click the **Save** button.

You are returned to the Route List screen, where after a few seconds the Destination settings are updated.

Starting, Stopping, and Deleting a Destination Node

You may start or stop a destination node on either the Route List screen or the Edit Route page:

Route List screen   Edit Route page

On the Route List screen:

1. Expand the route by clicking the ➤ icon.
2. Click the ▶ or ■ icon to start or stop the destination, respectively.

3. Click the **Confirm** button to confirm your action.

Route List screen   **Edit Route page**

On the Edit Route page:

1. Locate the desired destination to start or stop at the bottom of the page.
2. Either, click the ▶ or ■ icon to start or stop the destination, respectively.
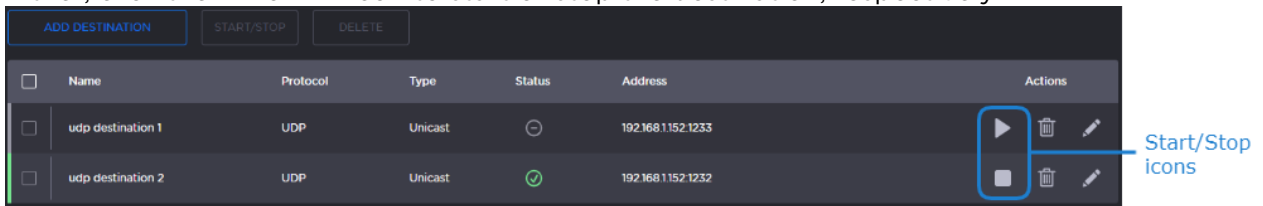
Or check the checkboxes next to each destination you wish to start/stop, and click the **Start/Stop** button.
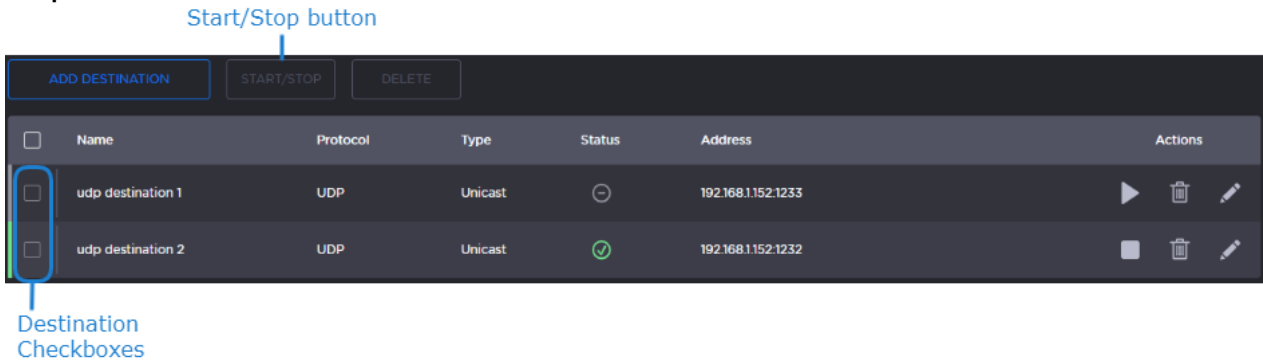
3. Click the **Confirm** button to confirm your action.

To delete a destination node:

1. On the Route List screen, click on the desired route to open the Edit Route page.
2. On the Edit Route page, locate the desired destination to delete.
3. Either, click the 🗑 icon at the end of the listing to Delete the corresponding destination.
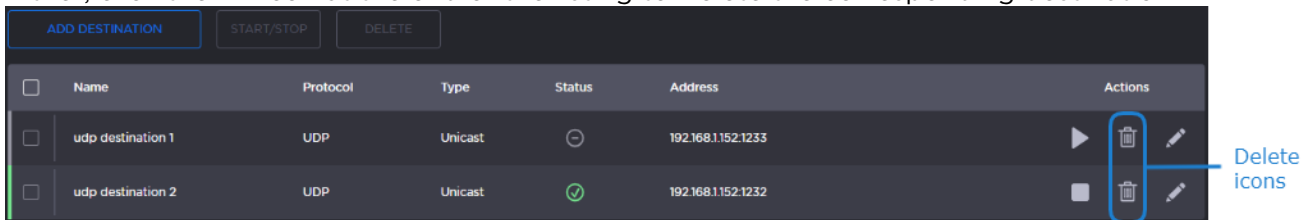
Or check the checkboxes next to each destination you wish to delete, and click the Delete button.

Delete button

Destination
Checkboxes
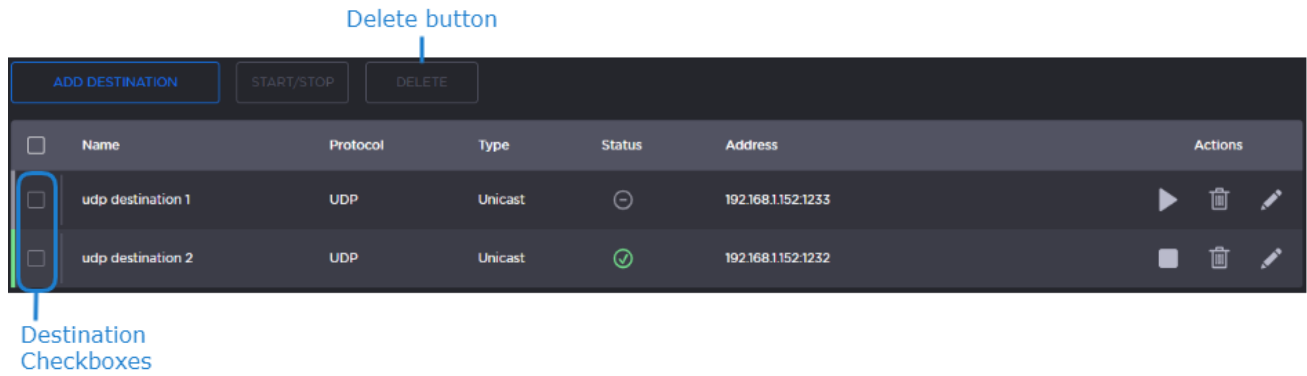
4. Click the **Confirm** button to confirm the deletion.

Performing Admin Tasks

The following content explains how to manage Media Gateway/SRT 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 and SRT Gateway**.

Topics Discussed

- **Media Platform**
- **Exporting and Importing Presets**
- **Accounts**
- **Certificates**
- **Licensing**
- **Network**
- **Security**
- **Update**
- **Reports (Logs)**
- **System Activity and Details**

Media Platform

> ⚠ **Important**
>
> Haivision SRT Gateway is not meant for multi-site Haivision Media Platform workflows. The following sections apply to Haivision Media Gateway only.

Media Platform-Media Gateway integration is used to distribute video to distant site locations, typically pairing a single Haivision Media Platform server with Haivision 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 is illustrated in the following figure:
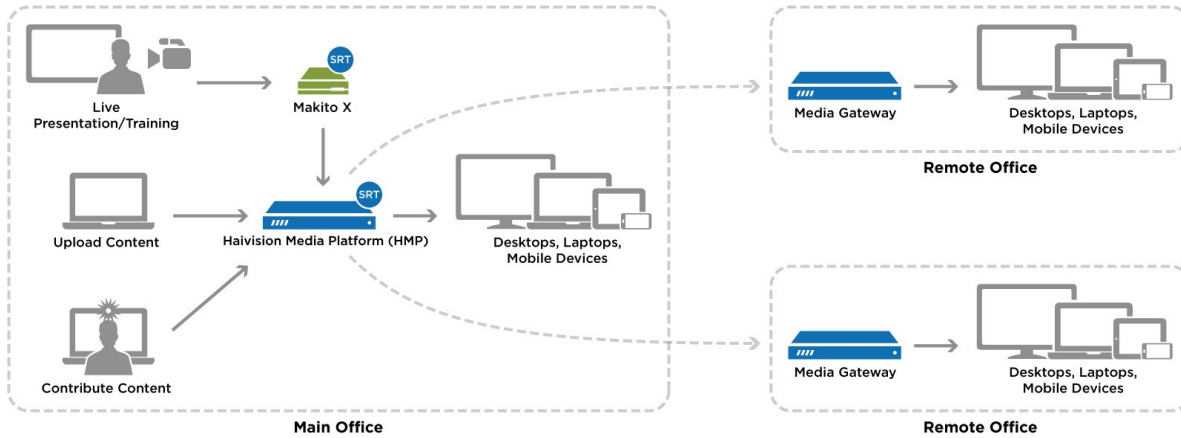
Pairing Media Gateway with a Media Platform Server

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**
- **Acquiring a Pairing Passcode**
- **Pairing the Devices**

Refer to your Haivision 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.
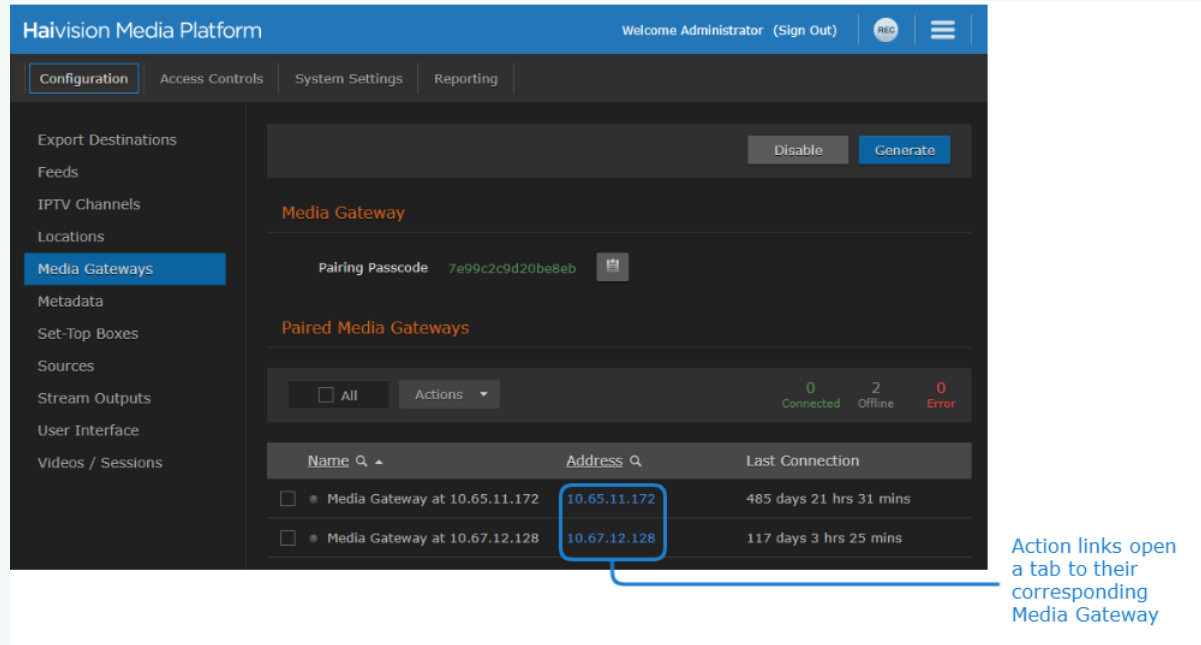
Acquiring a Pairing Passcode

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 **Configuration** in the admin toolbar and 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 port. 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.

> **Tip**
>
> In production environments, Haivision recommends using an FQDN when pairing a Media Gateway to a Media Platform.

In your browser tab of the Media Gateway you wish to pair with the Media Platform:

1. In the side menu under Administration, click **Configuration**.
2. Click **Media Platform** in the navigation toolbar.
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 FQDN 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:

- **Hostname/IP Address** — the FQDN 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.
- **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.

> ✅ 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, see the text next to the status icon or use the following:

⊘	Connected (Poll requested succeeded within the last 5 minutes).
⚠	Warning (Some potentially transient error).
⊖	Disconnected (Last poll response was received over 5 minutes ago).
🚫	Error (Last poll request failed due to authorization, 404, or pairing timeout).
✳	Pairing in progress.
✳	Disconnection in progress.

2. The Media Platform screen also tracks the connection's duration in the Last Connection field.
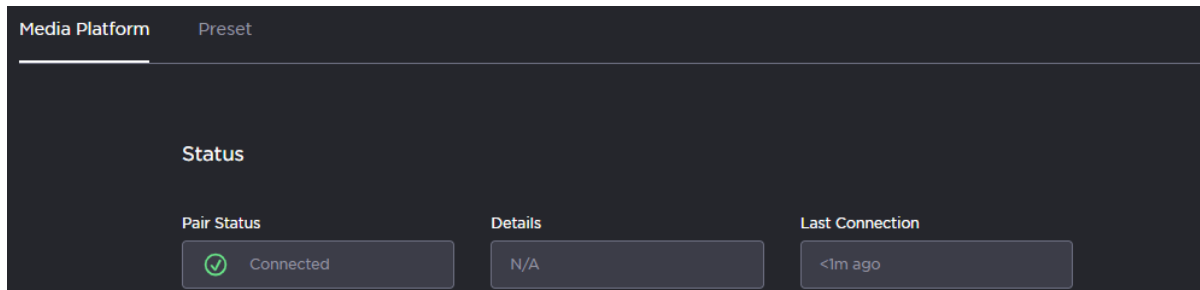
Blocking New Media Gateway Connections

To block any new Media Gateway connections:

1. In your Media Platform browser tab, click the ☰ icon and click **Administration**.
2. Click **Configuration** in the admin toolbar and 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, in the side menu under Administration, click **Configuration**.
2. Click **Media Platform** in the navigation toolbar.
3. Change one of the settings, such as update the "Identify As" name to something new.
4. Click **Update** for the new information to update 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, the pairing status returns to "Not paired", and the text boxes in the screen are cleared.

To clear the pairing settings:

1. In your Media Gateway browser tab, in the side menu under Administration, click **Configuration**.
2. Click **Media Platform** in the navigation toolbar.
3. Click the **Clear** button.
4. Click **Confirm** that you want to clear the pairing settings.

Disconnecting from a Media Platform Server

To disconnect from a Media Platform server:

1. In your Media Gateway browser tab, in the side menu under Administration, click **Configuration**.
2. Click **Media Platform** in the navigation toolbar.
3. Click the **Disconnect** button.
4. Click **Confirm** to verify that you want to disconnect from Media Platform.

Exporting and Importing Presets

The Preset 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.

Exporting a Preset   Importing a Preset

To export a preset:

1. In the side menu under Administration, click **Configuration**.
2. Click **Presets** in the navigation toolbar.
3. To export a preset of the current routes configurations, click **Export Preset**.

The browser downloads a .hmg file.

Exporting a Preset   **Importing a Preset**

To import a preset:

> ⚠ **Important**
>
> Importing a preset overwrites existing routes on the system.

1. In the side menu under Administration, click **Configuration**.
2. Click **Presets** in the navigation toolbar.
3. 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, a warning message appears in the view pane.
4. Click the **Import** button to start importing.
5. After the upload is complete, the file is validated for the following:
   • Correct file extension (.hmg).
   • Correct JSON format.

- Contains 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.

If an error occurs, an error message is displayed. If validation passes, then it starts applying the preset.

6. While the system is applying the preset, a message "Applying preset..." is displayed.
7. When complete, a message appears showing the number of routes created.

Accounts

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

> ⚠ **Note**
>
> Default passwords for each account are provided in the *Important Notice* document that is shipped with your hardware, or available on the Support Portal.

To view the available user accounts:

1. In the side menu under Administration, click **Access Control**.
2. Click **Accounts** in the navigation toolbar.

The available accounts are listed grouped by their roles. The account names and roles assigned to the accounts cannot be changed.

Role	Account Name	Description
Administrator	haiadmin	All access rights and administrator privileges.
Operator	operator	All rights to create and configure routes. Does not include rights to the administration screens.
Observer	user	Read-only access to the system. Does not include the rights to the administration screens.
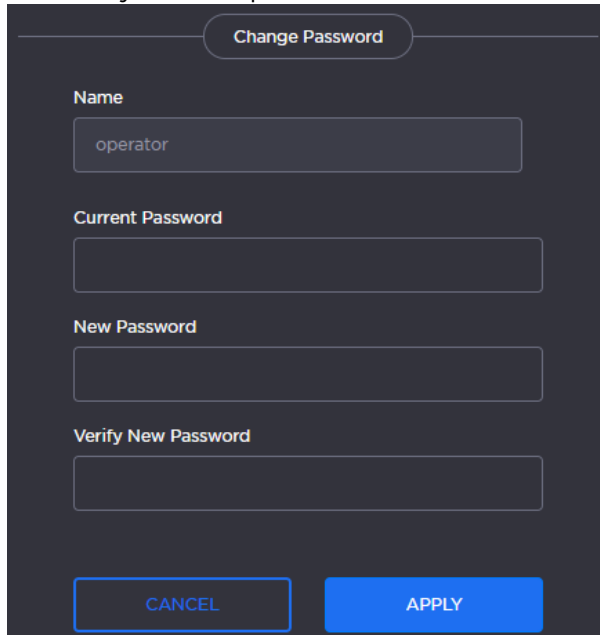
Changing an Account's Password

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. In the side menu under Administration, click **Access Control**.
2. Click **Accounts** in the navigation toolbar.
3. Click **Change Password** next to 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` and `hvroot` password can only be changed in the Console UI. See **Using the Console UI with Haivision Hardware** for details.

Certificates

From the Certificates page, you can generate an 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 available Identity Certificates. 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. In the side menu under Administration, click **System Settings**.
2. Click **Certificates** in the navigation toolbar.
   The Certificates page lists all generated certificate signing requests. The active certificate is indicated with a blue check.
3. Click the **Generate** button.

4. On the Generate Certificate or Private Key dialog that appears:

a. Enter a name for the certificate.
b. Esure the Type is Certificate Signing Request and fill in the remaining fields. See **Certificate Settings**.
c. For the Subject, click the ✏ icon and enter information about the device that the Identity Certificate represents. For more information, see the Subject entry in **Certificate Settings**. Click the **Apply** button.

5. Click the **Apply** button.
6. Returning to the Certificates list, click the link for the generated CSR to open the file in another window. 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). See **Importing and Activating a Certificate** to import the returned certificates.

> ✅ **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 and exported for signing.

Importing and Activating a Certificate

To import and activate a certificate:

1. In the side menu under Administration, click **System Settings**.
2. Click **Certificates** in the navigation toolbar.
3. Click the **Import** button.
4. On the Import 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**.
   c. If your certificate is encrypted, enter the password.
   d. Drag and drop or click **Browse** and select the CA-signed certificate (.crt extension) returned from the certificate request generated in the previous section.

5. Click **Apply**.
6. 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.
7. Click **Reboot** for the new active certificate to take effect.

Generating and Importing a Private Key

Generate a Private Key   **Import a Private Key**

To generate a private key:

1. In the side menu under Administration, click **System Settings**.
2. Click **Certificates** in the navigation toolbar.

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**.

5. Click the **Apply** button.
6. In the Certificates page, the newly imported certificate is added to the list and should have a green status LED. Click in the Active column to activate the certificate.
7. Click **Reboot**.

Generate a Private Key   **Import a Private Key**

To import a Private Key:

1. In the side menu under Administration, click **System Settings**.
2. Click **Certificates** in the navigation toolbar.
3. Click the **Import** button.
4. On the Import Certificate or Private Key dialog:
   a. For the Type, select **Private Key + Certificate Pair**.
   b. Enter the password for the private key.

c. To update your security certificate, drag and drop or click **Browse** and select the new Certificate and Private Key, and optionally a Intermediate Certificate Bundle file.

5. Click the **Apply** button
6. On the Certificates page, the newly imported files are added to the list. Click in the Active column to activate the certificate.
7. Click **Reboot**.

Generating a New Self-Signed Certificate

If you are upgrading to HMG/HSG version 3.2 or greater, due to a new restriction of TLS certificates in certain operating systems, a new self-signed certificate with a 2-year expiration should be generated after the upgrade. See "Cannot Access Web Interface from a Computer after an OS Update" in **Known Issues and Solutions** for more details on the issue.

To generate a new self-signed certificate:

1. In the side menu under Administration, click **System Settings**.
2. Click **Certificates** in the navigation toolbar.
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. Fill in the remaining fields. See **Certificate Settings**.
   d. Click the **Apply** button.

5. The new certificate is added to the Certificates list.
6. Select the new certificate in the Active column to activate it.
7. Optionally, delete the old certificate.
8. Click **Reboot** for the change to take effect.

Certificate Settings

The following table lists the configurable 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	Enter a unique name under which the certificate will be listed on the Certificates 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 added to the list of certificates. Clicking on the name of the request in the list opens it in a new browser window for copying the content into a CA application. After the request is signed by a CA the resulting certificate can be imported into HMG/HSG.
Digest Algorithm	Select the digest algorithm (Secure Hash Algorithm): SHA-256, SHA-384, or SHA-512.
Subject	The Subject identifies the device being secured, in this case, the Media Gateway/SRT Gateway. Clicking the ✎ icon opens a dialog to assist in properly formatting the subject. • Country • State (or province) • Location • Organization • Organizational Unit • 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 or Private Key	
Type	Select the certificate type: • Certificates: (Identify/CA-chains/Bundles) • Private Key + Certificate Pair
Name	(Certificates only) Name of the certificate.

Certificate Setting	Description
Format	(Certificates only) 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.
Private Key	(Private Key + Certificate Pair only) Select the file to upload.
Bundle File	(Private Key + Certificate Pair only) Select the file to upload.

Licensing

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

> ⚠ **Important**
>
> • Without a valid license key, you can sign in. However, you won't be able to create or edit routes until you have imported a license.
> • Adding a license server requires administrator privileges and a license key.

When a system is not licensed, the Route List page displays a License Required warning dialog. If the user's role is administrator, the dialog displays an **Add License** button.

Adding a License

To add a license:

1. After signing into the web interface, if you see a License Required dialog, click **Add License.**
   -or-
   In the side menu under Administration, click **System Settings**. Then, click **Licensing** in the navigation toolbar.
2. The Licensing view pane shows status information for the installed license, including its expiration date, version limit, product edition, and the status of other licensed options, as shown below:
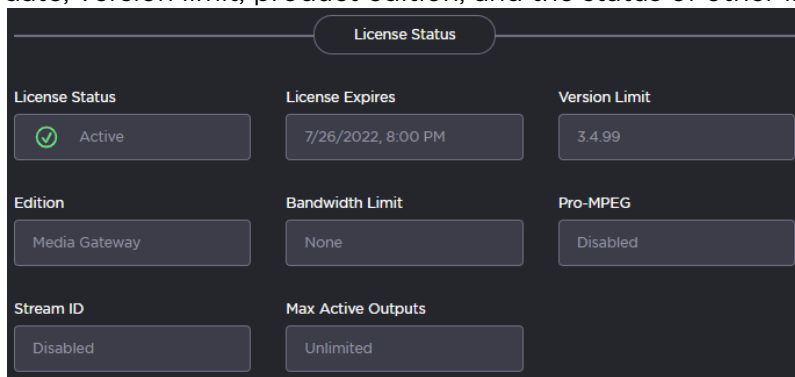
3. At the bottom of the screen, click the **Copy to Clipboard** copy your hardware details to the clipboard.

4. To request a license for your product:
    a. Log in to the Haivision Support Portal (https://support.haivision.com).
    b. After logging in, click **License Requests**.
    c. Click the **New** button.
    d. Select the appropriate device type and click the **Next** button.
    e. Fill in the form with the appropriate information, and click **Save**.
        Your license request is submitted and you will be contacted by a Haivision representative shortly with a license key for your product.
5. After you receive a license key, paste the license string in the New License text box.
6. Click **Update License** to load the license.

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

Related Topics

-   Viewing the Status of a License

Viewing the Status of a License

The license status screen includes the expiration date, version limit, product edition (Haivision Media Gateway or Haivision SRT Gateway), and other licensed options as shown in the table below.

	Haivision Media Gateway	Haivision SRT Gateway
Bandwidth limit (Mbps)	100, 200, 500	100, 200, 500
RTP PRO-MPEG FEC	—	Enabled
SRT Stream ID	—	Enabled

To view the status of a Media Gateway license:

1. In the side menu under Administration, click **System Settings**.
2. Click **Licensing** in the navigation toolbar.

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

Related Topics

-   Adding a License

Viewing the Version Number

There are three different ways to view the current version of your software:

Preferences/About   System Activity   Update

1. In the side menu **Preferences/About**.
    The About dialog opens to display the version information for the current installation.
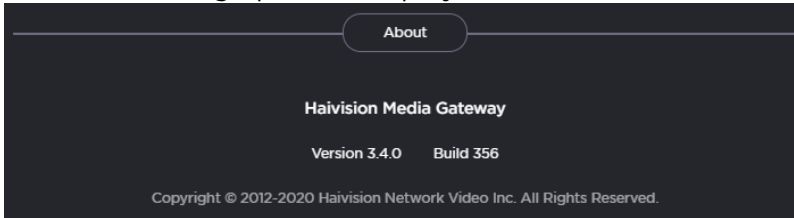
2. When finished, click **Close** to exit the dialog.

Preferences/About   **System Activity**   **Update**

1. In the side menu under Administration, click **Reporting**.
2. Click **System Activity** in the navigation toolbar.
    The version is listed under Hardware Info.
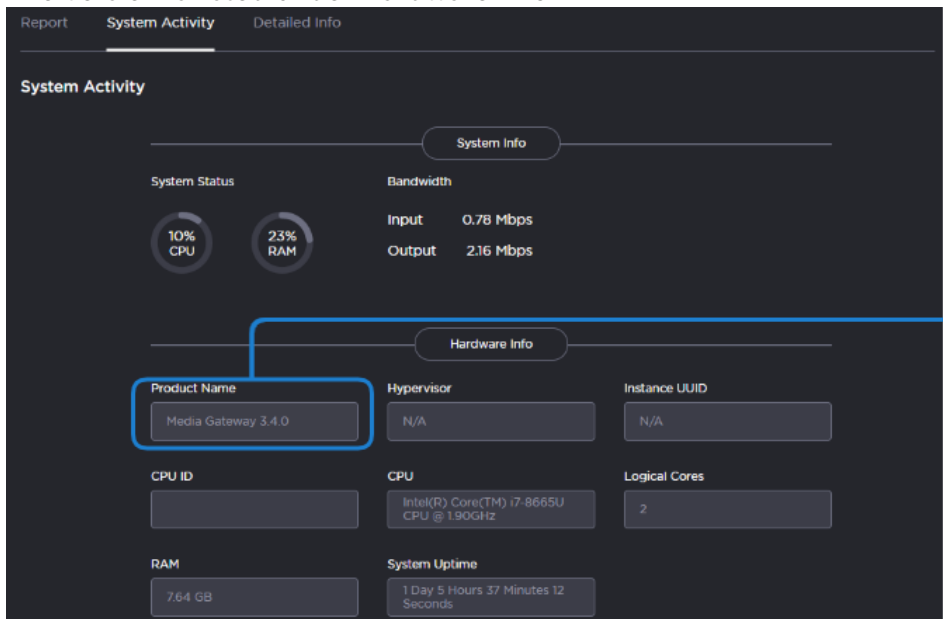
Preferences/About   **System Activity**   **Update**

1. In the side menu under Administration, click **System Settings**.
2. Click **Update** in the navigation toolbar.
    The version is listed under Installed Bundle.
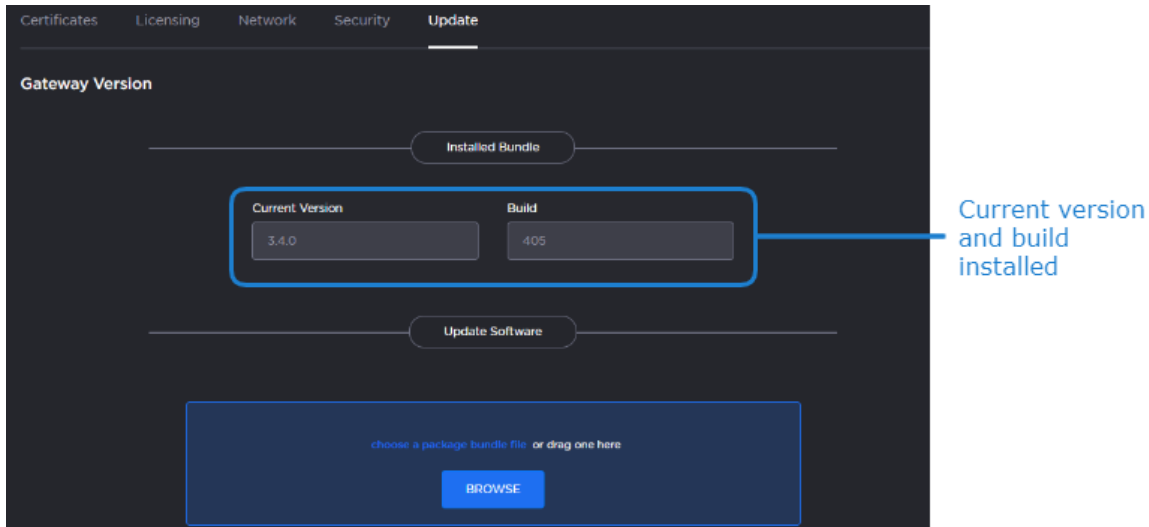
Related Topics

- **Downloading System Updates**
- **Installing an Update Package**

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. In the side menu under Administration, click **System Settings**.
2. Click **Network** in the navigation toolbar.
   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** for more information

   > ✅ **Tip**
   >
   > If DHCP is selected, the auto-assigned values appear in the IP address, Subnet Mask, and Gateway textboxes.

4. To configure multiple network interfaces, after you complete eth0, select the next interface (for example, eth1) and repeat the configuration.

   > ⚠️ **Note**
   >
   > Depending upon your device, the network interface prefixes may differ.

5. To add a bond interface, see **Creating a Bonded Interface** for more information.

6. To add a static route, under Static Routes click the **Add** button and provide the necessary data in the Add Static Route dialog.
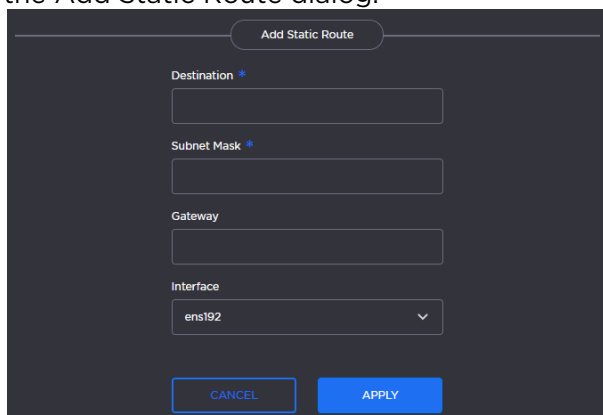
7. Click **Apply**. The route is added to the Static Routes listing on the Network Configuration screen.
8. Click the **Save Settings** button.
9. Click the **Reboot** button to have your network configuration changes take effect.

Network Settings

General   Interfaces   Static Routes

Network Setting	Description
General	
Hostname	The hostname to be assigned to the server. Specify the hostname as a fully-qualified domain name (FQDN). For example: myserver.mycompany.com
Default Interface	Select the default Ethernet interface. For new systems, this setting is unset by default.
NTP Server	(Optional). If the Network Time Protocol (NTP) is enabled, enter the IP address of the NTP server.
DNS Servers	(Optional). The Internet Protocol version 4 (IPv4) addresses of the Domain Name Servers to use.
Search Domains	(Optional). The search strings to use when attempting to resolve domain names.
RP Filter Mode	(Advanced users only) Reverse path filtering mode, as defined in IETF RFC3074 *Ingress Filtering for Multihomed Networks* . Currently, the recommended practice per RFC3074 is to use strict mode to prevent IP spoofing from DDOS attacks. If you are using asymmetric routing or other complicated multi-NIC routing, the default setting of Strict mode may cause system network outages and DHCP-enabled interfaces may be unable to obtain an IP address. • Strict mode: Each incoming packet is tested against the FIB and if the interface is not the best reverse path the packet check fails. By default failed packets are discarded. • Loose mode: Each incoming packet's source address is also tested against the FIB and if the source address is not reachable via any interface the packet check fails.
SNMP	Enable/Disable Simple Network Management Protocol (SNMP).

Network Setting	Description
Read-Only Community	SNMP string to be used when making read-only information requests.
SNMP Trap Servers	IPv4 or FQDN of a server and the Community Name to send SNMP traps to.

General   **Interfaces**   **Static Routes**

Network Setting	Description
Interfaces	
eth0 | eth1 | eth2 | ...	Allows for multiple interfaces. Select the appropriate tab to view and configure. ⚠ **Note** Depending upon your device, the network interface prefixes may differ.
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.
IP Address	Displays the IP Address. This is a unique address that identifies the unit in the IP network. 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. 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. 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.
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).

Network Setting	Description
Bonding Mode	(Bond Interface only) Modes for the Linux bonding driver determine the way in which traffic sent out of the bonded interface is actually dispersed over the real interfaces. Modes 0, 1, and 2 are by far the most commonly used among them. • Round Robin Sequential: Transmits packets in first available network interface (NIC) slave through the last. This mode provides load balancing and fault tolerance. • Active Backup: Only one NIC slave in the bond is active at a time. A different slave becomes active only when the active slave fails. This mode provides fault tolerance. • XOR Sequential: Transmits based on XOR formula. (Source MAC address is XOR'd with destination MAC address). This mode selects the same NIC slave for each destination MAC address and provides load balancing and fault tolerance. • Broadcast – Fault Tolerance: Transmits network packets on all slave interfaces. This mode is least used (only for specific purpose) and provides only fault tolerance. • IEEE 802.3ad Dynamic Link Aggregation: Creates aggregation groups that share the same speed and duplex settings. Utilizes all slave network interfaces in the active aggregator group according to the 802.3ad specification. This mode is similar to the XOR mode above and supports the same balancing policies. The link is set up dynamically between two LACP-supporting peers. • (Adaptive) Transmit Load Balancing (TLB): The outgoing traffic is distributed according to the current load and queue on each slave interface. Incoming traffic is received by one currently designated slave network interface. If this receiving slave fails, another slave takes over the MAC address of the failed receiving slave. • (Adaptive) Active Load Balancing (ALB): This includes balance-tlb + *receive load balancing* (rlb) for IPV4 traffic. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the server on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different clients use different hardware addresses for the server.
Slave Interfaces	(Bond Interface only) Select the checkboxes next to the interfaces to enslave it to the bond interface.

General **Interfaces** **Static Routes**

Network Setting	Description
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. 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. In the side menu under Administration, click **System Settings**.
2. Click **Network** in the navigation toolbar.
3. Verify that the correct interface (for example, eth0) is currently selected.
4. Click the **Bond Interface: Add** action link.
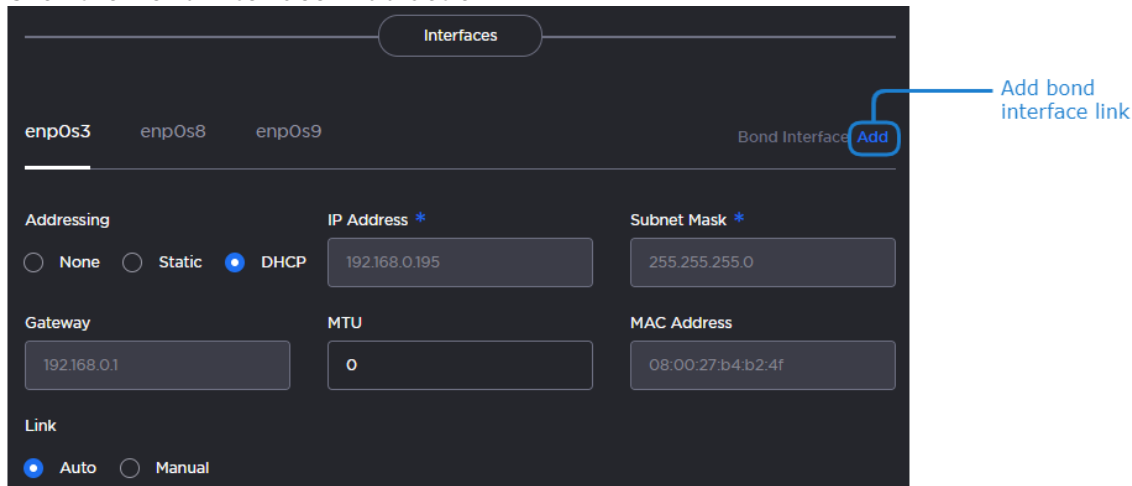
The bond0 tab appears and the **Bond Interface: Remove** action link replaces the **Add** action link.
5. In the Default Interface drop-down menu, select **bond0**.
6. Clink the **bond0** tab to reveal the bonding-specific fields (such as Bonding Mode and Slave Interfaces) and set as appropriate. See **Network Settings** for more information.
7. Click the **Save Settings** button.
8. Click **Reboot** to have your changes take effect.

Removing a Bonded Interface

To remove a bonded interface:

1. In the side menu under Administration, click **System Settings**.
2. Click **Network** in the navigation toolbar.
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.

Security

When setting up Media Gateway/SRT Gateway, you may configure additional security settings. Changing any of these settings requires a reboot.

- **FIPS:** Applies cryptographic modules accredited under the U.S. Federal Information Processing Standard (FIPS) Publication 140-2.

- **High Security (STIG) Environment:** Enables security hardening features for high-security environments, including:
  - Session timeouts/locks for all interfaces.
  - Stronger password requirements.
  - Lock/disable accounts due to multiple authentication failures or expired passwords.
  - Disabling unnecessary services.
- **Web Server:** Enables/Disables SSL protocols and ciphers.
  - Available TLS (Transport Layer Security) versions accepted: TLS v1, TLS v1.1, TLS v1.2.
  - Available SSL Ciphers include various AES encryption ciphers.
- **Advisory Notice and Consent Banner:** You may also configure an Advisory Notice and Consent Banner to appear when users first access the web interface's and Console UI's log in screen. The banner is typically an advisory/warning notice the user must consent to before signing in. For example:

To configure appliance security:

1. In the side menu under Administration, click **System Settings**.
2. Click **Security** in the navigation toolbar.
3. To configure FIPS compliance toggle the **FIPS** button to On.
4. To configure your Haivision Gateway for use in a high-security environment, toggle the **High Security (STIG) Environment** button to On.
5. To enable/disable SSL protocols use the SSL Protocol checkboxes.
6. To add SSL ciphers, under SSL Ciphers click the ⊕ icon and select the desired cipher. To remove a cipher click the ✖ icon for each added cipher.
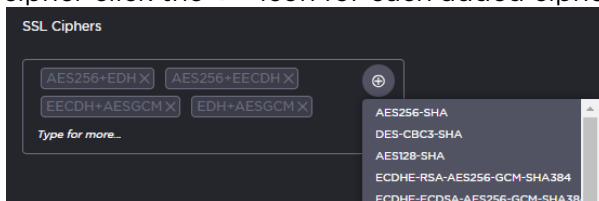
7. To configure a banner, toggle the **Advisory Notice** button to On, and enter the desired banner text in the Message textbox.
8. Click the **Save Settings** button.
9. Click the **Reboot** button to have your security configuration changes take effect.

Update

Before upgrading an appliance or VM, the update package must first be uploaded to the server.

> ⚠ **Note**
>
> To update cloud deployments (Amazon Web Services, Microsoft Azure, and Alibaba Cloud), the instance must be re-deployed using the new version. Upgrades cannot be installed using the standard web UI update process described in this section.

> ⚠ **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 in to the Haivision Support Portal at https://support.haivision.com.
2. Click the **Software Releases** link.
3. Under the Haivision Gateway heading, select the 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.

Proceed to **Installing an Update Package** to install the update.

Installing an Update Package

> ⚠ **Note**
>
> • Your system restarts after it installs the update.
> • You must disable the High Security (STIG) Environment option in the Security tab before installing the update. See Security for details.

To install the update package, after downloading it from the Haivision Support Portal as described in Downloading System Updates:
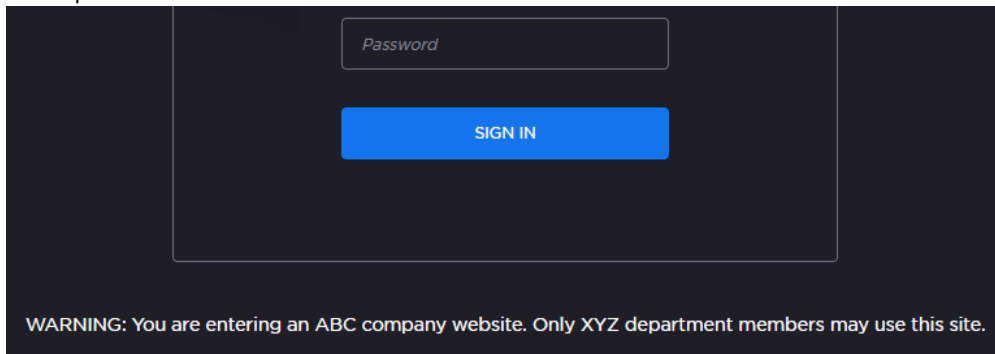
1. In the side menu under Administration, click **System Settings**.
2. Click **Update** in the navigation toolbar. The Update screen appears showing the currently installed version and build.
3. Click **Chose a file** and select the desired update bundle (.hai extension) and click **Open**.
   -or-
   Drag and drop the update bundle file from your desktop to the highlighted area on the Update screen.
4. Verify that the bundle listed is the one you want to install, and click **Upload**.
5. When the bundle has been uploaded, click **Update**.
6. When prompted, click **OK** to confirm. Your system restarts after it has installed the update.

Reverting an Upgrade

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

> ⚠ **Note**
>
> If you have an appliance or server, you must perform this procedure at its physical location.

1. If applicable, attach a monitor, keyboard, and mouse to the appliance or server. (See **System 100 Appliance Quick Start Guide** or **Server Quick Start Guide** for connection details.)

2. Reboot the device. (See **Rebooting or Shutting Down** for instructions on rebooting via the Console UI.)
3. After the BIOS loads, when the following screen appears on the monitor immediately move the cursor to the previous version using the ↑ or ↓ arrow keys.

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

```
Haivision Media Gateway release 3.3.0-127
Haivision Media Gateway release 3.2.0-752




         Use the ↑ and ↓ keys to change the selection.
         Press 'e' to edit the selected item, or 'c' for a command prompt.
       The selected entry will be started automatically in 3s.
```
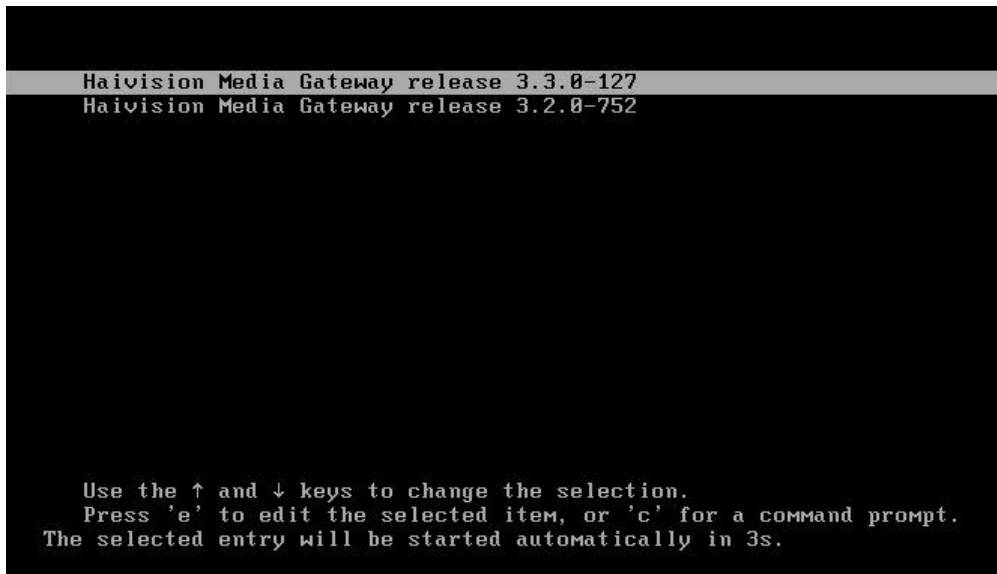
4. Ensure the previous version is selected, and press the **Enter** key.

After the system starts, you can try reinstalling the upgrade again or contact **Haivision Support** for assistance.

> ✅ **Tip**
>
>   If you choose not to upgrade again, subsequent reboots will require you to perform this procedure. Contact **Haivision Support** for instructions on changing the bootloader's default version.

Reports (Logs)

Media Gateway/SRT 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 System messages and Gateway logs, as well as files from `/var/log` and `/opt/haivision/madra`.
System Messages	Operating system messages. Includes `/var/log/messages`.

Log Name	Description
Haivision Gateway	Log data from the server processes, including: • `/opt/haivision/var/log/kulabyte/` — engine logs. • `/opt/haivision/var/log/system_snapshot.dat` — system snapshot.

Enabling Diagnostic Logging

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

To enable logging:

1. In the side menu under **Administration**, click **Reporting**.
2. Click **Report** in the navigation toolbar.
3. Toggle the Enable Diagnostic Logging button to On.
4. Confirm you would like diagnostic logging on in the confirmation dialog and click **Apply**.

> ⚠️ **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. In the side menu under **Administration**, click **Reporting**.
2. Click **Report** in the navigation toolbar.
3. The view pane consists of the Logs pane.
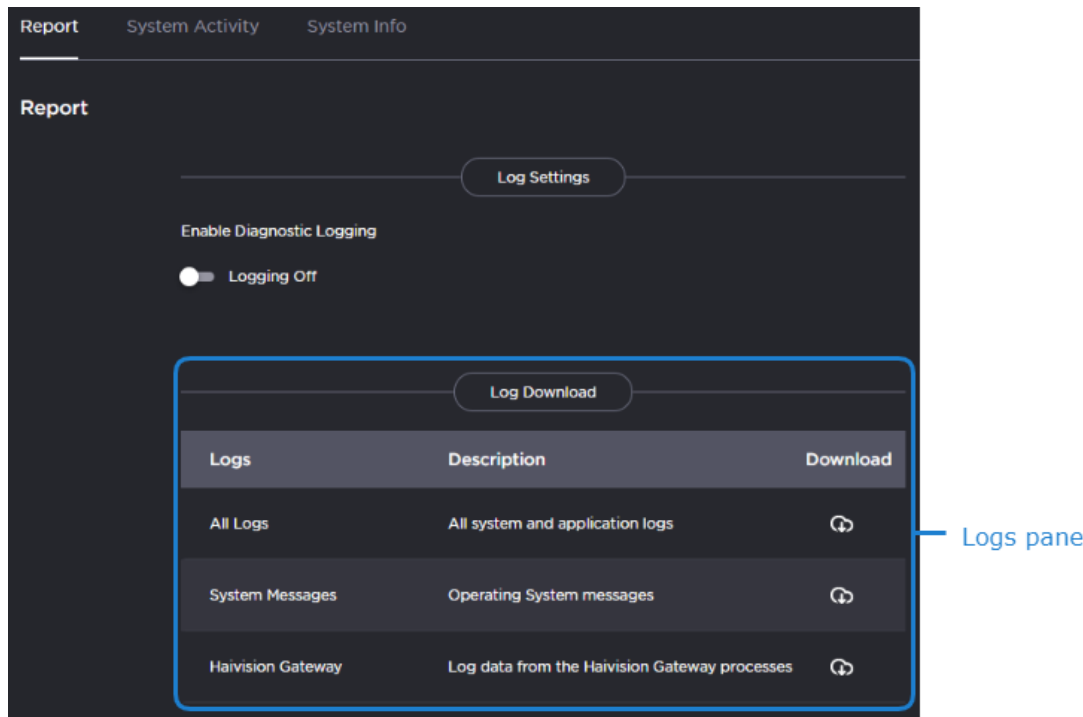
4. In the Logs pane, click the desired log's ⊕ icon to download a zip file of the log's text files.
5. If you select "All Logs," open the zip file and browse the folder structure:

```
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**
- **Viewing the Status of a License**
- **Downloading System Updates**
- **Viewing the Version Number**

System Activity and Details

The web interface includes dashboards to provide a quick view of the overall system health. 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. In the side menu under **Administration**, click **Reporting**.
2. Click **System Activity** in the navigation toolbar. The System Activity dashboard appears:

The System Info pane provides the following information:

- CPU usage
- Memory usage
- Input/Output network bandwidth

The Hardware Info pane provides the following information:

- Product edition and version

- VMware information (if applicable)
- CPU, number of logical cores, and RAM information
- Service tag and express service code (if using an Media Gateway/SRT Gateway server)
- System uptime

When paired with a Haivision Media Platform, the VOD Bandwidth pane appears and charts usage in Mbps.

- Clicking the items in the legend 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.
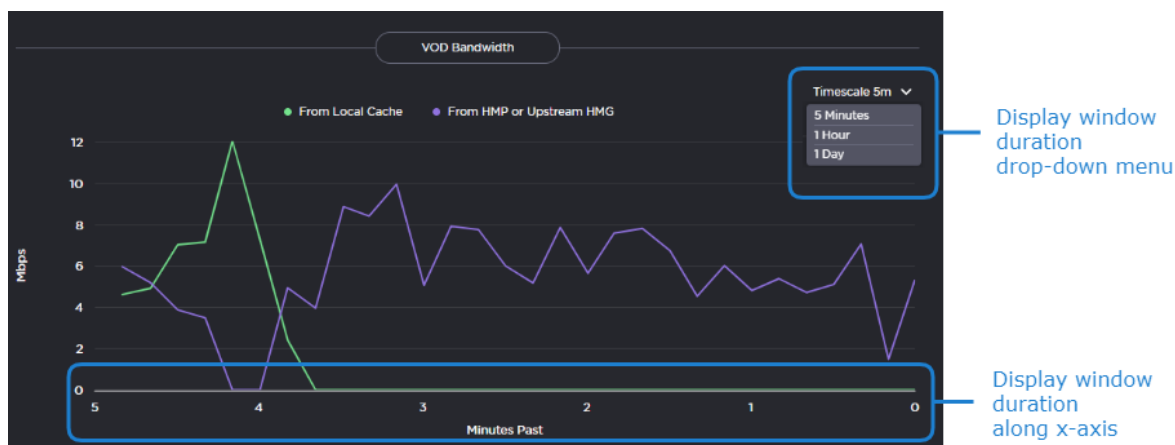
In the Disk Space pane, you see information regarding disk usage.

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

Click **Clear Video Cache** to delete cached video previously downloaded from HMP. When prompted to confirm, click **Clear**.

Related Topics

- **Viewing a Route's Statistics**
- **Reports (Logs)**
- **Clearing the Video Cache**

Viewing the Detailed Info Dashboard

To view graphs of the network bandwidth and CPU and memory usage:

1. In the side menu under **Administration**, click **Reporting**.
2. Click **Detailed Info** in the navigation toolbar. The Detailed Info dashboard appears:

Use the drop-down menus at the top of the window to specify the refresh rate and time scale for the graphs.

The refresh rate indicates how often the graph is updated and the time scale indicates the amount of time displayed on the graph. When the actual timeframe exceeds the specified time scale, 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.

Related Topics

*   **Viewing a Route's Statistics**

Clearing the Video Cache

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

To clear the video cache:

1. In the side menu under **Administration**, click **Reporting**.
2. Click **System Activity** in the navigation toolbar.

3. In the Disk Space pane, click the **Clear Video Cache** button to delete the cached video previously downloaded from Media Platform.
4. When prompted to confirm, click **Apply**.

Related Topics

- **Viewing a Route's Statistics**

Warranties

1-Year Limited Hardware Warranty

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

EXCLUSIONS AND LIMITATIONS

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

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

This warranty does not apply:

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

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

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

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

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

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

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

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

OBTAINING WARRANTY SERVICE

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

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

APPLICABLE LAW

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

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

EULA - End User License Agreement

READ BEFORE USING

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

Click the following link to view the Software End-User License Agreement: **Haivision EULA.pdf**

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

SLA - Service Level Agreement

1. Introduction

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

2. Definitions

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

3. Service Levels for the Video Content Management System

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

Type of Access	Definition	Availability Level
Write Functions	• Access to all functions through the administrative user interface. • Ability to add or modify objects and metadata through the application programming interface ("API") • Ability of ingest service to check for new or updated files or feeds	99.999%
Read-Only Functions	• Ability to retrieve data through the API • Ability for Audience Members to authenticate through the Access Service • Ability for Audience Members to play Published Media Objects • Ability for Audience Members to play Haivision VCMS-authenticated or entitled Published Media Objects • Ability to complete Transactions	99.999%

4. Exceptions to Availability for the VCMS

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

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

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

Type of Maintenance	Purpose	Write Functions Available	Read Functions Available	Maximum Time Per Month	Continuous Time in Mode (Max)	Window (Central Time)	Min Notice
Normal	• Preventive maintenance on the software/ hardware components of Haivision VCMS • Addition of new features/functions • Repair errors that are not immediately affecting Your use of Haivision VCMS	No	Yes	10 Hours	6 Hours	10:00pm - 5:00am	48 Hours
Urgent	• Repair errors that are immediately affecting Your use of Haivision VCMS	No	Yes	30 Minutes	15 Minutes	Any Time	3 Hours

Type of Maintenance	Purpose	Write Functions Available	Read Functions Available	Maximum Time Per Month	Continuous Time in Mode (Max)	Window (Central Time)	Min Notice
Upgrades	• Perform upgrades on software or hardware elements necessary to the long term health or performance of Haivision VCMS, but which, due to their nature, require that certain components of Haivision VCMS to be shut down such that no access is possible	No	No	1 Hour	1 Hour	12:00am - 4:00am M-F	5 Days

5. Credits for Downtime for the VCMS

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

6. Support Services for the VCMS

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

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

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

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

7. Service Levels for Haivision Streaming Media Service

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

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

Agents and Polling Frequency

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

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

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

8. Credits for Outages of Haivision Streaming Media Service

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

9. No Secondary End User Support

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

Getting Help

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